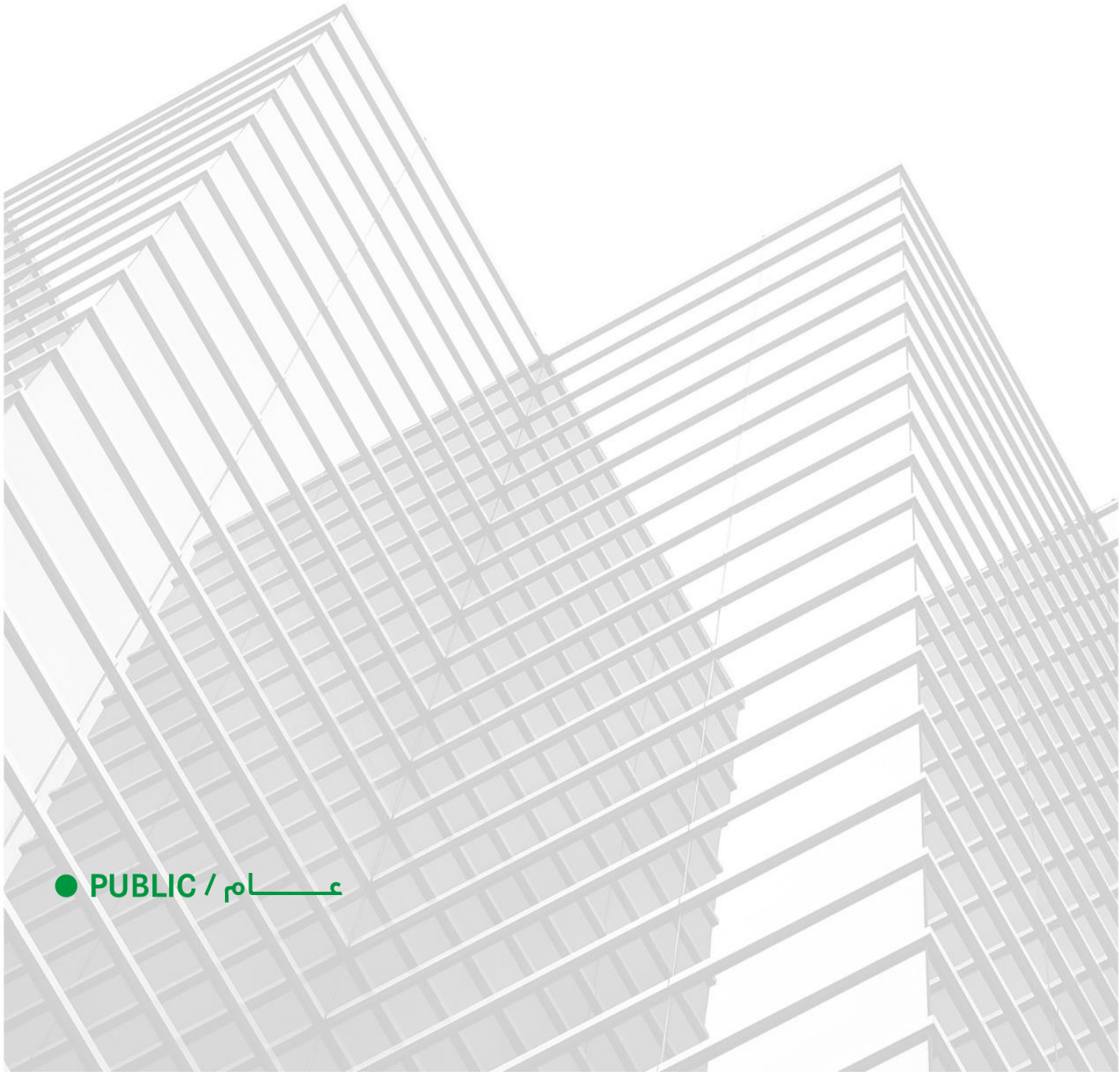
دائـــرة الـصـحـــة
DEPARTMENT OF HEALTH

Guidelines for the Implementation of Abu Dhabi Healthcare Information and Cyber Security Standard



PUBLIC / عـــــام

Document Title	Guidelines for the Implementation of Abu Dhabi - Healthcare Information and Cyber Security
Document Ref. Number	DOH/GL/ICSO/ADHICS/V2/2024 Version: V2
New/Revised	Revised
Publication Date	May, 2024
Effective Date:	August, 2024
Document Control:	Department of Health (DOH) - The Health Sector Regulator in the Emirate of Abu Dhabi
Applies To:	Any entity Including but not limited to, Healthcare Facility, Payer, Healthcare Technology and Service Provider in the Emirate of Abu Dhabi that generate, access, store, use, process and/or transmit health information.
Owner:	DoH Information & Cyber Security Office
Revision Date:	Three years from publication date
Revision Period:	May, 2027
Contact:	Abu Dhabi Healthcare Information Security Program aamen@doh.gov.ae

1.Guideline Purpose and Brief

1. Introduction

The Department of Health (DoH) has established the Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard to mandate entities on how to protect confidentiality, integrity and availability of Health Information and effectively manage information security risk by implementing suitable policies, procedures, and technical controls.

The adoption of ADHICS Standard by entities will facilitate secure usage of medical technology and exchange of information maintaining public trust in healthcare operations and Government initiatives towards Healthcare Information Exchange (HIE).

This is the revised implementation guidelines to help entities in the implementation of ADHICS V2.0 controls and requirements effectively.

2. Legal Background

The Federal Law No. (2) for the year 2019 on the use of Information and Communications Technology (ICT) and The Federal Law No. (45) of the year 2021 on Data Privacy mandates security and privacy of Health Information.

Implementing the ADHICS standard will significantly improve the entity information security risk profile but does not exclude the entity from any legal liabilities.

3. Purpose of this Document

This document aims to provide a common set of guidelines to help DoH in scope entities in the development, implementation, establishment and maintenance of security and data privacy requirements set by ADHICS Standard to protect the healthcare information under their control.

The healthcare sector is becoming the biggest target for malicious actors. As health Information becomes digitalized and healthcare equipment more and more 'connected', the risks are exponentially rising. Compromise of healthcare systems can have significant consequences, including breaches of confidentiality, financial losses, and even threats to patient safety. The implementation of the standard will create an environment that can add new technologies and techniques in a controlled way without significantly adding to the entity risk environment. Aligning security with entity operations will not only protect patient safety and privacy but will also ensure continuity of effective delivery of high-quality care by mitigating disruptions that can have a negative impact on healthcare operations and clinical outcomes.

Healthcare delivery is often time critical. Unstructured information security controls can add delays to healthcare delivery. The Standard's holistic approach covers the whole organization not just IT, and encompasses people, processes, and technology across the lifecycle of health information. This enables employees to readily understand risks and embrace security controls as part of their everyday working practices without introducing significant delays.

This guideline interprets "how" the controls mentioned in the ADHICS Standard can be implemented. Therefore, the primary focus is on the domains, controls, and sub-controls of Section B of the ADHICS Standard. For ease of use, the numbering system of Section 4 of this guideline matches Section B of the Standard.

Note that this document is only an implementation guideline and does not override ADHICS or any other regulatory documents issued by the DoH or other government entities. In case of contradiction, please refer and follow the standard.

It is the entity's management responsibility to implement and maintain Health Information security and privacy.

4. Scope

This guideline is applicable to all types and sizes of entities that are mandated to be compliant with ADHICS as per the timelines defined by DoH.

The ADHICS standard applies to any/all Information Technology systems and applications fully owned by in scope entities , as well as the third party systems or partners system accessible by the entity to store and process Health Information and support healthcare operations, and any other Information Technology system and application utilized within Abu Dhabi Healthcare ecosystem e.g. Shafafiya portal, Malaffi, the (Healthcare Information Exchange platform), DoH e-Services, Medical Tourism portal, etc.

The applicability of specific control mandates/requirements of the Standard is defined based on the maturity, operational complexity, and risk environment of the implementing entity. Section A-2 of the standard explains the applicability of the controls.

5. Partnership

The National Cybersecurity Strategy envisages a partnership across Government, Public and Private sectors to achieve excellence in cybersecurity.

The ADHICS Standard is intended to build the entity's capability to secure its information assets and continue functioning and delivering its healthcare activities without interruption. At the same time, a comprehensive set of technical security services are also being provided to the healthcare sector by DoH to contain and limit exposure to information security threats. These include Awareness E-Learning branded as Health Sector Cyber Learning Program and technical services such as 24*7*365 security incident management, vulnerability & technical assessment security advisories, newsletters, forensic assessment and a threat intelligence platform (Brand & Digital Asset Monitoring) providing actionable threat intelligence feeds to entities, specific to their deployed assets branded as the Abu Dhabi Health SOC.

This will leverage the investments, resources, and technologies of DoH to reduce the risk exposure across the Abu Dhabi Healthcare sector.

For more information on or support from Abu Dhabi Healthcare CERT - Contact (24/7):

soc@doh.gov.ae (or) +971 2 4193 777

For more information and support on the Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard - Contact:

ADHICS@doh.gov.ae (or) +971 24193612

---

2. Definitions and Abbreviations

No.	Term/Abbreviation	Definition
2.1	**ADHICS**	Abu Dhabi Healthcare Information and Cyber Security Standard
2.2	**ADMCC**	Abu Dhabi Monitoring and Control Centre
2.3	**BC**	Business Continuity
2.4	**BIA**	Business Impact Analysis
2.5	**BYOD**	Bring Your Own Device
2.6	**CAB**	Change Advisory Board
2.7	**CAPA**	Corrective Action and Preventive Action
2.8	**CCTV**	Closed-circuit television
2.9	**CE**	Continuing Education
2.10	**CEO**	Chief Executive Officer
2.11	**CPD**	Continuing Professional Development
2.12	**CSP**	Cloud Service Provider
2.13	**CSIRT**	Computer Security Incident Response Team
2.14	**DMZ**	Demilitarized zone
2.15	**DoH**	Department of Health
2.16	**DoS**	Denial of Service
2.17	**DPIA**	Data Privacy Impact Assessments
2.18	**DPO**	Data Protection Officer
2.19	**DPA**	Data Processing Agreement
2.20	**DR**	Disaster Recovery
2.21	**EMR**	Electronic Medical Record

2.22	**FTP**	File Transfer Protocol
2.23	**HIE**	Health Information Exchange
2.24	**HIIP**	Healthcare Information Infrastructure Protection
2.25	**HR**	Human Resources
2.26	**HTTPS**	Hypertext transfer protocol secure
2.27	**ICT**	Information and Communications Technology
2.28	**ICU**	Intensive Care Unit
2.29	**IT**	Information Technology
2.30	**ISGC**	Information Security and Governance Committee
2.31	**IDS**	Intrusion Detection System
2.32	**IPS**	Intrusion Prevention System
2.33	**ISMS**	Information Security Management Systems
2.34	**IPR**	Intellectual Property Rights
2.35	**LAN**	Local Area Network
2.36	**MDM**	Mobile Device Management
2.37	**MitM**	Man in the Middle
2.38	**MCC**	Monitoring and Control Centre
2.39	**NAC**	Network Access Control
2.40	**NDA**	Non-Disclosure Agreement
2.41	**NTP**	Network Time Protocol
2.42	**PACS**	Picture archiving and communication system
2.43	**PEDs**	Personal Electronic Devices
2.44	**PHI**	Protected Health Information
2.45	**PII**	Personally Identifiable Information

2.46	**RTO**	Recovery Time Objective
2.47	**RPO**	Recovery Point Objective
2.48	**SC**	Service Continuity
2.49	**SDLC**	Software Development Lifecycle
2.50	**SEIM**	Security Event Information Management
2.51	**SLA**	Service Level Agreement
2.52	**SFTP**	Secure File Transfer Protocol
2.53	**SPF**	Sender Policy Framework
2.54	**SIMDB**	Security Incident Management Database
2.55	**SOC**	Security Operations Center
2.56	**TLS**	Transport Layer Security
2.57	**UAE**	United Arab Emirates
2.58	**UPS**	Uninterruptible Power Supply
2.59	**VPN**	Virtual private network
2.60	**WAN**	Wide Area Network
2.61	Adversaries	Person or group contending against another
2.62	Asset Custodian	Employee within an organization who is responsible for physically safeguarding and maintaining an asset. The asset custodian is responsible for the day-to-day management of physical IT assets, such as computers, servers, and mobile devices. They are responsible for ensuring that these assets are properly stored, maintained, and accounted for throughout their lifecycle. They are accountable for the physical security and maintenance of the asset.

2.63	Asset Owner	An asset owner is the individual or department within an organization who is responsible for managing a particular asset throughout its lifecycle. The asset owner is responsible for making decisions about the asset, such as when to upgrade or replace it, ensuring that it is properly maintained, secured, and used effectively to achieve the organization's goals.
2.64	Assets	Data or images collected and stored (in a digital or hard copy format) and the information systems that are used to generate, collect, store, or exchange these data or images and/or support in entity operations for care delivery.
2.65	Authentication	Establishing that an agent using a computer system is the agent in whose name the account is registered.
2.66	Availability	Information is accessible and useable on demand by authorised entities.
2.67	Back up (verb)	To make a copy of data for the purpose of recovery.
2.68	Backup (noun)	The process of backing up refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. A backup and the associated procedures and processes can only be verified once the restore procedures and process have been confirmed via an actual restore.
2.69	Business Continuity Plan (BCP)	Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.
2.70	Classification	Accords different levels of protection based on the expected damage, prejudice and/or loss the health information might cause in the wrong hands.
2.71	Cloud Environment	Computer resources housed in a distant data center and controlled by a cloud services provider, such as programs, servers (both physical and virtual), data storage, development tools, networking capabilities, and more.
2.72	Confidentiality	Information is not available or disclosed to unauthorised individuals, entities, or processes.

2.73	Cryptography	The science of coding and decoding messages so as to keep these messages secure. Coding (encryption) takes place using a key that ideally is known only by the sender and intended recipient of the message. Cryptographic control is the ability to render plain text unreadable and re-readable using cryptographic techniques. Such techniques are also used to ensure integrity and non-repudiation.
2.74	Custodian	In the health information security context, a custodian is a person in an appointed role that is entrusted with the custody or care of a person's health information. An entity may have custodianship over health care information.
2.75	Data integrity	Data must not be altered or destroyed in an unauthorised manner and accuracy and consistency must be preserved regardless of changes.
2.76	Data Privacy Impact Assessment (DPIA)	Assessing the potential impacts on privacy of a process, information system, program, software module, device or other initiative which processes protected health information for taking actions as necessary to treat privacy risk.
2.77	Data Subject	A natural person about whom the entity holds protected health information and who can be identified, directly or indirectly, by reference to that information.
2.78	Disaster recovery (DR)	Disaster recovery is the process, policies and procedures related to preparing for recovery critical to an organisation after a natural or human-induced disruptive event. Disaster recovery planning is a subset of a larger process known as business continuity management (BCM). This includes planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. Disaster recovery planning is a subset of a larger process known as business continuity management (BCM). This includes planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure.

2.79	Disruptive event	Any event, regardless of cause, that disrupts (or has the potential to disrupt) an organisation's ability to maintain identified critical functions.
2.80	Environmental (threats/hazards)	Threats or risks of physical harm. From an IT security viewpoint this is to do with physical access to or potential physical risks to hardware.
2.81	Facility	A single physical location from which health goods and/or services are provided. A health care organisation may consist of multiple facilities.
2.82	Firewall	A device or set of devices configured to permit, deny, encrypt or proxy all computer traffic between different security domains based upon a set of rules and other criteria.
2.83	Health information	Information regarding the health of a subject of care in physical and/or computer-processable form. It can be present as text, video, audio, photos, and images.
2.84	Health Information Exchange (HIE)	Malaffi - that safely and securely connects public and private healthcare providers in the Emirate of Abu Dhabi.
2.85	Health Sector Entity	Herein referred to as "entity" Including but not limited to, Healthcare Facility, Payer, Service Provider in the Emirate of Abu Dhabi that generate, access, store, use, process and/or transmit health information.
2.86	Healthcare Facility	A facility or organisation providing patient health care services, including services to promote health, to protect health, to prevent disease or ill-health, treatment services, nursing services, rehabilitative services, or diagnostic services.
2.87	Healthcare Technology and Service Providers	Any external party that provides medical device, system, application, infrastructure or database, both individually or collectively that generate, access, store, use, process and/or transmit health information.
2.88	Key Management	Key management refers to management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding, and replacement of keys.
2.89	Malware	Software developed for malicious intent. This includes viruses, worms, adware, Trojan horses, key-loggers.

2.90	Media	Any technology used to place, keep, transport and or retrieve data. This includes both electronic devices and materials as well as non-electronic options e.g., paper.
2.91	Medical device	An article, material, instrument, implant, software, apparatus, or machine to be used, alone or in combination for the prevention, diagnosis or treatment of illness or disease, or for detecting, measuring, restoring, correcting or modifying the structure or function of the body for some health purpose. Typically, the purpose of a medical device is not achieved by pharmacological, immunological, or metabolic means. Some medical devices have the capability to collect, record data and to transmit over the internet and to other devices that are equipped to receive said data.
2.92	Medical equipment	Medical devices requiring calibration, maintenance, repair, user training, and decommissioning – activities usually managed by clinical engineers. Medical equipment is used for the specific purposes of diagnosis and treatment of disease or rehabilitation following disease or injury; it can be used either alone or in combination with any accessory, consumable, or other piece of medical equipment. Medical equipment excludes implantable, disposable or single-use medical devices.
2.93	Patient / Subject of care	One or more persons scheduled to receive, receiving, or having received a health service.
2.94	Payers	Insurers, Third Party Administrators and Brokers that provide operational services such as health insurance, Claims processing, Policy benefits management etc.
2.95	Portable media	Media that can be used to transport electronic information independently of a network. This includes floppy disks, USB storage, portable hard-drives and other devices that have a data storage mechanism (cameras, cell phones, iPods etc.).
2.96	Procedure	A specification or series of actions, acts or operations which must be executed in the same manner in order to always obtain the same result in the same circumstances (e.g., emergency procedures).

2.97	Professional	An individual who is engaged in a health care related occupation.
2.97	Personally Identifiable Information (PII)	Personally identifiable information (PII) is any data that could potentially identify a specific individual.
2.98	Protected health Information (PHI)	Protected health information (PHI), also referred to as personal health information, is the demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.
2.99	Recovery Point Objective (RPO)	Point in time to which data are to be recovered after a disruption has occurred.
2.100	Recovery Time Objective (RTO)	Period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions are to be recovered after a disruption has occurred.
2.101	Risk management	The identification, assessment, and prioritization of risks including using resources to minimize, monitor, and control the impact of these risks.
2.102	Secure Coding	The practice of developing software that is safeguarded from security vulnerabilities.
2.103	Service level agreements (SLA)	A formally negotiated agreement between two parties that records the common understanding about services, priorities, responsibilities, guarantee, and such collectively, the level of service.
2.104	Standard	Unless specified otherwise, the term refers to ADHICS Standard.
2.105	Supply Chain	The sequence of processes involved in the production and distribution of a product or a service.
2.106	Systems	Applications or electronic business processes which support the collection, access, processing, and exchange of health information.
2.107	Telehealth	The use of electronic information and communication technologies to support long-distance virtual clinical healthcare practice, patient and professional health-related education, public health, and health administration.

2.108	Teleworking	A work arrangement in which employees are able to have flexibility in their working location. That is: a central place of work is supplemented by a remote location (e.g., home), usually with the aid of information technology and communications.
2.109	Virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user. Viruses usually corrupt or modify files on a targeted computer.

3.Guideline Content

Section 1

Steps

This section is the starting point of the Guidelines listing the different steps needed for implementation to be followed in the same order. Each step is covered in detail in the subsequent sections.

Steps

Step 1	**Obtain a copy of the standard**	The standard is available for free download from DoH website. (www.doh.gov.ae > Initiatives & Programs > AAMEN)
Step 2	**Know your Entity type**	Pharmacy, Clinic, Centre, Hospital, Insurer, Broker, TPA and Healthcare Technology and Services Provider etc.
Step 3	**Identify the control applicability**	Basic, Transitional, Advanced or Service Provider (Refer Section A.6 of the Standard)
Step 4	**Mandatory Requirements**	Refer Section 2 of this document
Step 5	**Baseline Policies**	Refer Section 3 of this document
Step 6	**Controls Implementation**	Refer Section 4 of this document
Step 7	**Useful Forms & Templates**	Refer Section 5 of this document
Step 8	**Continual Improvement**	Refer Section 6 of this document
Step 9	**Compliance & Reporting**	Refer Section 7 of this document
-	**Baseline checklists**	Refer Section 8 of this document

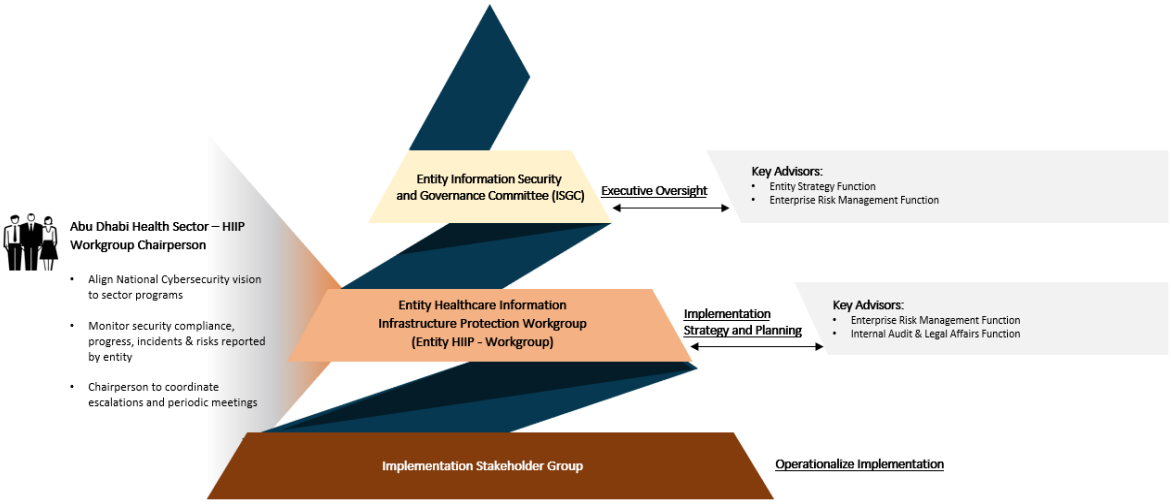
Section 2

Mandatory Requirements

This section provides guidelines for the implementation of the mandatory requirements defined in Section A of the ADHICS Standard.

1. Governance

The entity, regardless of its type, shall implement the three-layer ADHICS Governance pyramid structure specified in Section A-3 of the Standard, as applicable.



This is to assign ADHICS implementation roles and responsibilities and ensure separation of duties. The three layers correspond to the entity management (ISGC), information security management (HIIP) and the implementation team (ISG). Please refer to the standard for details of the roles. Existing entity committees can also fulfill these roles where suitable.

The Implementation stakeholders' group can have third party staff. However, the other two groups should comprise of entity or parent entity staff as applicable. The committees of the ADHICS Governance pyramid in the standard can be scaled down to match smaller entities provided the three roles are defined. The memberships of the three groups as well as their meetings should be documented and retained for audit purposes.

The HIIP workgroup will be the interface between the entity and the of the DoH as well as between the entity management and implementation teams.

Within the ADHICS Governance pyramid, this guideline is primarily intended for the use of the HIIP workgroup and implementation stakeholders' group and should always be referred to in combination with the corresponding parts of the ADHICS standard.

2. Risk Management

Risk Management including assessment and mitigation requirements of ADHICS are covered in Section A-4 of the Standard. An entity should conduct Information Security Risk Assessment at least once in a year or whenever changes to their environment to identify and monitor the risks.

The outcome of the Risk assessment can be used by the entity to determine the level of effort and resources needed to protect entity's information assets. The results of periodic risk assessments must be aligned with the implementing entity's priorities, initiatives and investments.

The organization is required to establish a comprehensive procedure for identifying, analyzing, and mitigating the risks associated with the utilization of information technology, processes, and personnel. This procedure should incorporate a Risk Acceptance criterion.

The risk management procedure components are as follows:

1. **Identification of Assets:** Identify the "crown jewels" of your entity, such as data, systems, or other information assets.
2. **Identification of Vulnerabilities:** Identify weaknesses and deficiencies in entity's systems/processes could put confidentiality, integrity, and availability of the entity at risk.
3. **Identification of Threats:** Identify major potential causes of assets or information becoming compromised.
4. **Identification of Existing Security Control:** Mention the controls you already have in place to address the identified vulnerability and threat by mitigating it or reducing the likelihood and/or impact.
5. **Risk Evaluation:** Identify risk and its level for each identified asset by combining the information acquired about the asset, the associated vulnerabilities, and the existing security controls in place.
6. **Risk Ownership:** Determine the risk owners who are responsible for ensuring that risks are handled/mitigated as appropriately and within a certain time frame.
7. **Risk Treatment:** Select suitable treatment options from the following, as required:
    - **Risk Reduction:** Applying suitable controls to reduce risk.
    - **Risk Acceptance:** Accepting the risk based on entity's risk acceptance criteria.

- **Risk Avoidance:** Avoiding the activity causing risk.
- **Risk Transfer:** Transferring risk to another party

8. **Ongoing Risk Review:** Perform periodic Risk assessments to monitor and review to ensure that the security controls implemented continue to be appropriate and effective and ensures that any changes within the environment have not impacted the control effectiveness.

3. Information Security Policies

The development and application of Information Security policies and procedures, additional or as required by the ADHICS Standard is the responsibility of the implementing entity.

To facilitate the policy development process for entities, sample Baseline Policies are provided in Section 3 of this document. Entities are free to customize the provided baseline policies as per their risk environment as long as they remain compliant with the requirements of the ADHICS Standard and any other applicable DoH or legal requirements.

4. Asset Classification

Section A-6 of the ADHICS Standard defines the asset classification scheme to be used within the entity. Asset management policy and processes are covered in Domain 2 – Asset Management of Section B. Controls AM 1 to AM 3 and associated sub-controls cover asset classification. Guidelines are available under the corresponding parts of this document.

Information assets includes information/data in all its form, as well as the underlying application, technology, and physical infrastructure to support its accessing, processing, storing, communicating, and sharing. Information assets include, but are not limited to:

- Information (in physical and digital forms)
- Medical device and equipment used for diagnosis, therapy, monitoring, rehabilitation, and care etc.
- Applications and system software's
- Network infrastructure devices
- Services and processes
- Information systems

- Virtual infrastructure
- Physical infrastructure (Data center, servers, access barriers, electrical facilities, HVAC systems, etc.)
- Human resources (in support of services/care delivery)

Section 3

Baseline Policies

This section consists of templates for the basic information security policies required for the effective implementation of the identified and applicable controls within an entity.

Entity can customize to suit its purposes taking into account inclusion of all required information as per its operating and risk environment. Or the entity may use its own policies if already in place as long as they adequately reflect the requirements of the ADHICS standard. The term ‘Users’ herein means all employees, third parties and vendors who access the entity information in any form.

Index

1. Information Security High Level Policy

Objectives

The objective of this Policy is to outline the basic principles of protecting all the information assets of **[Entity Name]** and make all Users within the Entity aware of the potential security threats and associated business risks.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, information, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. The **[Director or job title assigned with responsibilities of Entity's higher management]** of **[Entity Name]** shall endorse this policy for its effective implementation.

Policy Statement

[Entity Name] is committed towards securing the confidentiality, integrity and availability of information for the day-to-day business operations. The security of information and other assets is therefore regarded as fundamental for the successful business operation of **[Entity Name].**

This high-level information security policy is a key component of **[Entity Name]**'s overall information security management framework and should be considered along with **[Entity Name]**'s specific and more detailed information security policies, procedures, standards, and guidelines.

Adherence to this policy will help to protect data/ information of **[Entity Name]** and its customers from information security threats, whether internal or external, deliberate or accidental.

It is recognized that detailed policies and procedures will be required and **[Entity Name]** is committed to implementing these in full.

Core Principles

[Entity Name] recognizes that secure operations are dependent upon securing three core organizational elements, which are people, process and technology. Thus, all **[Entity Name]** activities must adhere to the general principles laid down. This policy acts as an umbrella document to all other security policies and associated documents. This policy defines the requirements to:

1. Maintain the confidentiality, integrity and availability of information, and information assets.
2. Meet the UAE regulatory, statutory and legislative requirements.
3. Assure a secure and stable information technology (IT) environment.
4. Identify and assign the security roles and responsibilities for coordinating the implementation of security across the entity.
5. Report and investigate all suspected information security related breaches.
6. Provide appropriate information security training & awareness to all employees (permanent & contract employees).
7. Ensure employees/contractors/third parties are aware of the entity's Information security policies.
8. Design appropriate controls and procedures to support the implementation of this Information Security Policy.

9. Ensure all stakeholders are responsible for implementation of respective security policies and procedures within their area of operation and oversee adherence by their team members.
10. Continually improve information security through implementation of corrective and preventive actions.
11. Prepare, maintain and test business continuity plans in a practical manner based on the business needs.
12. Periodically review this Policy for adequacy and appropriateness.

Policy Compliance

1. Any violation or breach to the policy may be subject to information security violation management process and/or HR disciplinary procedure, the Code of Conduct for employees and any other applicable UAE Laws in this regard.
2. Compliance with **[Entity Name]** policies is a pre-requisite condition of all employment or vendor contracts. Non-compliance creates the potential for legal actions that may significantly impact **[Entity Name]** operations, including possible damage to our business assets or reputation.
3. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from [Information Security Section/Department or the function assigned with information security responsibilities].
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
5. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

2. Human Resource Security Policy

Objectives

To ensure right resources are hired and utilized to support secure delivery of organizational objectives and services and are relieved in a manner that does not impact organizational assets, value, reputation and financial conditions any time current or in future.

Scope

This policy is applicable to all **[Entity Name]** Users and covers all type of information and information processing facilities.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. The **[HR section/department or the function assigned with HR responsibilities]** of **[Entity Name]** is responsible to ensure compliance to the defined security controls in the policy.

Policy Statement

Note: Human resources management must comply with applicable UAE laws and their amendments, the HR Security Policy and controls defined by **[Entity Name]**, and any other relevant regulations followed by the entity in this context.

Prior to Employment

Screening

The **[Manager of Human Resources or the job title assigned with responsibilities of managing human resources]** shall ensure the following primary checks as part of the screening process, including but not limited to:

a) Verification of personal data such as date of birth

b) Availability of satisfactory character references

c) Check (for completeness and accuracy) of the applicant's curriculum vitae.

d) Confirmation of claimed academic and professional qualifications.

e) Verification of previous employment data

f) Independent identity check (Emirates ID or passport or similar document)

g) An assessment of background, by seeking criminal records verifications through the official sources, as applicable for the role

h) Primary Source Verification Report, as applicable

Legal and Contractual Requirements

1. The **[HR section/department or the function assigned with HR responsibilities]** shall ensure that as part of contractual obligation, employees shall agree and sign the terms and conditions of an employment contract.
2. The **[HR section/department or the function assigned with HR responsibilities]** shall ensure that the terms and conditions of employment contract include statements relevant to information security such as (but not limited to):

   a) Performance of daily activities in compliance with the Information security and all other relevant policies, procedures and standards.

   b) Extended responsibilities beyond the department premises, outside normal working hours and after employment tenure.

3. The **[HR section/department or the function assigned with HR responsibilities]** shall ensure that all employees are aware and have acknowledged on the non-disclosure clauses included in their

employment contract which extends beyond the employment with **[Entity Name]** and are aware & have read and acknowledged the information security policies of **[Entity Name]**.

4. The **[HR section/department or the function assigned with HR responsibilities]** shall review and update any existing contract/agreement with employees, contractors and third-party users, as required.

During Employment

Employees Awareness and Training

1. The **[HR section/department or the function assigned with HR responsibilities]** in coordination with the **[Information Security Section/Department or the function assigned with information security responsibilities]** shall ensure that information security and privacy awareness programs are conducted for new employees as part of an induction program and records are retained.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** in coordination with **[HR section/department or the function assigned with HR responsibilities]** shall ensure that relevant awareness programs are conducted on a regular basis, to raise and maintain the employee awareness with regard to information security and Privacy.
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** shall develop an annual information security and privacy awareness and training plan that establishes culture of continuous awareness through innovative methods, as required.
    - Internal training portals – e-learning modules covering best practices, etc.
    - Periodic Emails, Manuals, Guidelines and Handbooks
    - Wallpapers/Screensavers/Posters
    - PowerPoint Presentations
    - Conducting quiz and survey.
4. The **[HR section/department or the function assigned with HR responsibilities]** shall ensure active participation and tracking of completion of training and awareness session.
5. The **[Information Security Section/Department or the function assigned with information security responsibilities]** shall review and update the content of the awareness material periodically to:

a) Present current risks around the healthcare industry, and ways to address it.

b) Lessons learnt from the recent incidents if any.

c) Demonstrate the need to protect Health Information

d) Include benefit of information security and privacy compliance

e) Demonstrate stakeholders' responsibilities.

f) Demonstrate practices for operating all information assets in a secure manner.

g) Highlight entity, government and regulatory demands.

Disciplinary Process

1. The **[Manager of Human Resources or the job title assigned with responsibilities of managing human resources]** in coordination with [Information Security Manager or the job title assigned with responsibilities of managing information security] shall ensure that non-compliance with the information security policies, procedures and standards are investigated and disciplinary measures are enforced.
2. Any serious misconduct or significant violation of information security policies shall be referred to the Entity Disciplinary Committee or the designated person for further action.
3. The formal disciplinary actions shall be decided considering the following factors:

   a) Nature and gravity of the breach

   b) Its impact on business

   c) Whether it's a first or repeat offence

   d) Whether the violator was properly made aware and trained

   e) Relevant legislation

   f) Employment contract etc.

Termination or Change of Employment Role

1. Information systems access shall be revoked effective the date of issuance of termination order.

2. The concerned person logical and physical access to **[Entity Name]** facilities and information system shall be withdrawn.
3. All information assets issued to the concerned person shall be returned with immediate effect and prior to settlement of dues and departure from **[Entity Name]**.
4. The **[Manager of Human Resources or the job title assigned with responsibilities of managing human resources]** shall ensure that a formal procedure in place to intimate all resignations and termination to effectively revoke access to information systems and applications on a timely manner.

   Where necessary, the conditions of extended confidentiality agreements, releases, and waivers of liabilities shall be made post-employment applicable to the departing employee, contractor, vendor, or other third-party user.

Policy Compliance

1. Any violation or breach to the policy may be subject to information security violation management process and/or HR disciplinary procedure, the Code of Conduct for employees and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

3. Information Assets Management Policy

Objectives

32Asset Management encompasses planning, demand, acquisitions, usage, maintenance, and disposal of information assets in order to achieve efficient and effective service delivery.

This policy's objective is to ensure that the Information Assets used and/or held by **[Entity Name]** are managed, controlled, secured, and utilized in an effective and efficient manner.

Information assets includes information/data/systems in all its form, as well as the underlying application, technology, and physical infrastructure to support its processing, storing, communicating, and sharing. The following are considered information assets:

- Information (in physical and digital forms)
- Medical device and equipment used for diagnosis, therapy, monitoring, rehabilitation, and care etc.
- Applications and Software
- Information System
- Network Infrastructure Devices
- Services and Processes
- Physical Infrastructure (Data center, servers, access barrios, electrical facilities, HVAC systems, etc.)
- Mobile and Portable Devices
- Human resources (in support of services/care delivery)

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, information, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. All information assets owners are responsible for:
    a) Ensuring that this policy is applied within their area of their responsibility.
    b) Ensuring that information assets associated with information processing facilities are appropriately classified.
    c) Defining and periodically reviewing access restrictions and classifications, considering applicable access control policies

Policy Statement

Information Assets Management

1. The **[Entity Name]** shall maintain an asset inventory by including information, hardware, Bio-medical and software assets.
2. Asset Owner shall be identified for each asset within the asset inventory.
3. An asset type must be defined for all types of information assets e.g., Hardware, Software, IT Infrastructure etc.

4. The asset inventory shall be reviewed and updated on a regular basis and as and when there is any major change in the entity's operating environment.
5. The entity shall retain the records of the review of periodic asset inventory.
6. The Entity shall create an Acceptable usage policy, communicated, and acknowledged by all users.
7. The entity shall restrict and control removable media devices as appropriately. Exemptions shall be authorized and relevant records to be retained.
8. All information assets shall have the following identified & documented, as applicable:
    - Asset ID
    - Asset Type/Type of device
    - Machine name/Device name
    - Manufacturer name
    - Date the asset was entered into the inventory.
    - Asset Classification
    - Serial number
    - IP address
    - Operating status
    - Physical Location
    - Function name
    - License information
    - Software version
    - Asset owner for each asset
    - Maintenance due date (PPM)
    - End of Life and End of Support
    - Distribution list/Access control list.

9. The asset inventory shall establish relations between various types of information assets, in support of care delivery.
10. Service A ➔ needs B Information ➔ supplied by C Device/Equipment/Process/Dependent-Service ➔ processed using D Application (ERP/EMR/Office Automation Applications/etc.) ➔ running on E Technology (server/systems) ➔ supported/operated/managed by XYZ Roles (human resources involved in care delivery)

Information Assets Classification Guidelines

1. The owners of the information assets shall be responsible for assigning/maintaining appropriate classifications based on the following criteria:
   a) Criticality and value of content/information it holds or carries.
   b) Intended Users of the information.
   c) Resulted risk impact if the information was accessed by unauthorized individuals.

Information Assets Classification Categories

1. Information assets of **[Entity Name]** shall be classified into one of the following classifications or as per **[Entity predefined classification scheme].** The classification is wholly based on the examination of the value of the information, who will have access to the information assets, and the resulting risk impact if the information was compromised or accessed by unauthorized individuals.

Classification Category	Description	Risk Impact	Examples
Secret C0 M100 Y100 K0 R227 G5 B19 # E30513 RED	Information that requires substantial and multilevel protection due to its highly sensitive nature. Disclosure of such information could have a serious and sustained impact upon the government, national security, social cohesion, economic viability and health of the nation.	The compromise of information in this category could result in significant damage to [Entity Name] financial status and reputation , critical system operations, customers trust and legal implication etc..,	VIP Health Information, Research and Proprietary Data, Intellectual Property

	Information disclosure could potentially threaten life or seriously prejudice public order.		
Confidential C0 M80 Y95 K0 R232 G78 B27 # E84E1B ORANGE	Information that requires robust protection due to its critical support to decision-making within the Entity, and across health sector and government. Information that could disclose designs, configurations or vulnerabilities exploitable by those with malicious intent. Information that the Entity, or through government or regulatory mandates, has a duty of care to others to hold in safe custody (e.g. critical personal information, health/Health Information, government information, financial information etc.).	The compromise of information in this category could result in damage to [Entity Name] competitive advantage, strategic operational plans, government relations, legal binding.	Strategic/Critical Projects Contracts, Personal Identifiable Information (PII), Protected Health Information, Health Information, Financial Information (Credit Card/Debit Card Details), Employee Payroll data, Budget information, management data, Audit reports, Risks registers, assets registers, Financial details in relation to projects or proposals, strategic/critical projects RFPs, HR Files, IP addresses, Network Architecture Diagrams,

			Information Security Incident Reports etc.
Restricted C100 M0 Y0 K0 R0 G158 B227 # 009EE3 BLUE	Information that must be afforded limited confidentiality protection due to its use in the day-to-day operations. Disclosure of such information could have limited adverse impact on the functioning or reputation of the Entity or the government. Information that relates to the internal functioning of the Entity and will not have general relevance and applicability to a wider audience. Although individual items of information are not sensitive, taken in aggregate they may reveal more information than is necessary, if they were to be revealed.	Disclosure of such information with unauthorized individuals could result in undesirable effect or minimal impact on [Entity Name] financial, operational or reputation status.	External Government Correspondences, Policies, Procedures, Standard Operating Procedures, Internal Circulars, contract of non-critical projects, projects charters, etc.
Public C100 M0 Y100 K0 R0 G150 B64 # 009640 GREEN	Information destined to be used in public domain or public use, and has no legal, regulatory or organizational restrictions for its access and/or usage. Intended purpose from the creation, access and use of the information is the general advancement of society, promotion of the interest of the organization and of the country, providing essential information equipping citizens, patients and other stakeholders understand better the country's/governmental/organizational vision and values.	No impact	Website information, news articles, marketing disseminations, etc.

2. Sharing of Information classified as Secret and Confidential with third parties or any other [Entity Name] employees shall be based upon obtaining proper authorization as defined previously and applying strict controls such as signing NDA.

Information Assets Tagging

Every Information asset (as applicable) should be tagged immediately after procurement. It is the responsibility of the [Information Technology (IT) Head or job titles assigned with responsibilities of managing Entity's Information technology section/department] for each business entity/location to ensure that all assets are accurately tagged and recorded in the asset inventory list before they are used on the network.

Information Assets Reclassification

1. Information Asset owner shall consider reclassification of the information asset at any point of time whenever there is a need to change the classification due to changing business requirements or based on the following:
    a) Change in the value of information.
    b) Changes to environment (location, access, storage, processing, usage, etc.)
    c) Changes in protection levels
2. The reclassification of assets shall be done by the information asset owner either in terms of degrading or upgrading its classification.
3. Since re-classification involves change in access control, appropriate pre-cautions/security controls shall be considered against information disclosure.

Information Assets Handling

1. All information assets shall be handled according to the assigned classification category of information.
2. The entity shall define operating procedures for handling medical devices as applicable.
3. Appropriate controls shall be in place to ensure security of the information during its transmission over different channels such as LAN, WAN, Internet or physical delivery. The level of controls shall be in line with the classification category of assets being transmitted.

4. The recipient of the information shall treat it in accordance with the information asset classification established by its originator.
5. The information asset owner shall consider proper transmission controls for the information assets transmission requirements.

Information Assets Disposal

1. Information Assets shall l be disposed (transferred or scrapped) if:
2. The equipment has reached end of life or end of support.
3. The equipment does not suit the computing environment requirement and cannot be upgraded further to meet the same.
4. The equipment has gone faulty and cannot be repaired or beyond economic repair.
5. The equipment is no longer needed to support health care delivery.
6. All kinds of information assets shall be disposed-off in a secure manner at the end of their intended life cycle with proper authorization from the information asset owner. The entity shall shred the paper based/physical records prior to disposal.
7. The information asset owner shall authorize and ensure that appropriate security controls are considered while disposing the information assets so that the information contained in it is irrecoverable by destroying the asset or sanitizing/wiping the asset The entity shall maintain the records of disposal. The records shall have fields, including but not limited to:
    - Information and/or asset owner
    - Type of media disposed.
    - Asset classification of the asset disposed.
    - Disposal type (secure erase, shredding etc.)
    - Reason for disposal
    - Data removed or not.
    - Disposal authorized by

Physical Media Transfer

1. Necessary authorization shall be obtained from the designated asset owner prior to transfer of any media.
2. Information-containment media must be shielded from unwanted access, misuse, and corruption when being transported outside of the physical bounds of the entity
3. Logs shall be maintained, to track dispatch and receipt, for physical media transferred; and
4. Authorized personnel shall be identified for movement of electronic media and software applications from onsite location to offsite location

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for employees and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from [Information Security Manager or the job title assigned with responsibilities of managing information security] on a case-to-case basis.

4. Physical & Environmental Security Policy

Objectives

To ensure that information assets receive adequate physical and environmental protection, and to prevent or reduce probabilities of physical and environmental control/security compromises (loss, damage, theft, interference, etc.), the following aspects of physical and environmental security shall be considered:

a) Physical protection of data center and information processing equipment(s)/facilities
b) Physical entry control for secure areas
c) Medical devices/equipment(s) protection
d) Heating, ventilation, and air conditioning of critical areas and workplaces
e) Supporting mechanical and electrical equipment's
f) Surveillance of critical areas and workplaces
g) Security and protection of physical archives
h) Fire and environmental protection
i) Visitor management

Scope

This policy is applicable to all **[Entity Name]** users, operating facilities, information technology (IT) resources including, IT teams, information, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for the development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.

4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. The **[Unit/Department assigned with responsibilities of physical building security]** shall be responsible of ensuring that maintenance and testing of fire detection and suppression systems is carried out on a periodic basis, and that records and reports of such testing are maintained.

Policy Statement

Physical Access Provisioning & De-Provisioning

1. Access to **[Entity Name]**'s premises will be granted as per the procedure of physical access of the Entity (to be developed by the Entity based on the business needs).
2. Visitors' access, including third party vendors, to **[Entity Name]** premises will be granted on case-by-case basis as per the Entity procedures.
3. De-Provisioning of physical access is valid under the following circumstances:
    a) End of employee's service, terminated and absconded.
    b) Vendors/Contractors completing their engagement or as per the expiration of the temporary gate pass.
    c) If requested by the Director of the department which the user belongs to.
    d) If User found to have violated the policy or misused the provided access in any mean.

Identification Cards

1. All employees shall wear the employee ID card issued by the [HR section/department or the function assigned with HR responsibilities] while they are inside the premises of **[Entity Name].**
2. All non-employees (contractors, consultants, suppliers, vendors, partners, etc.) shall wear respective identification cards while they are within the premises of **[Entity Name].**
3. The ID cards shall be placed in a manner that is clearly visible.

4. All new employees shall be primarily issued with temporary ID cards, till they are issued with their ID cards.
5. All Users shall return their ID card in the event of resignation, termination, transfer or retirement to **[HR section/department or the function assigned with HR responsibilities].**
6. All employees are authorized to politely challenge individuals who don't have ID cards while they are within the premises of **[Entity Name].**
7. The entity shall establish a reporting mechanism to handle the lost or stolen access cards.

Physical Access Control

1. Physical access to areas containing critical information and information processing systems shall be controlled and allowed for authorized Users only.
2. Entry to **[Entity Name]** premises shall be provided to visitors only after notifying the particular employee whom the visitor is asking to visit and verifying the purpose of visit with him/her.
3. The entity shall maintain a visitor access log register and shall record the details of visitors along with the user who has provided access to entity's premises.
4. Visitors shall be escorted at all times by authorized employee while in **[Entity Name]** premises.
5. Users shall refrain from entering critical areas without getting proper approval from authorized employee.
6. All areas that contain critical information and information processing facilities shall be fitted with strong physical access control mechanisms.
7. Physical access shall be deactivated or revoked for terminated Users.
8. Physical access rights of all Users shall be reviewed on a periodic basis (minimum once every six months) by the **[Information Security Section/Department or the function assigned with information security responsibilities]** in coordination with respective managers/directors responsible of critical information and information processing facilities in order to check if there are access rights that are no longer needed.
9. The names and designations of Users who have the right to authorize others to have access to areas that contain critical information or critical information processing facilities shall be maintained by the

[Information Security Section/Department or the function assigned with information security responsibilities] in coordination with the respective managers/directors.

10. Users shall keep their cabinets/drawers locked when leaving the offices at the end of the day.

Secure Working Areas

1. The entity shall define secure areas (e.g., Data Center, ICU, Narcotics room etc.) to ensure the access to those areas are controlled as appropriately with designated owners.
2. The **[Information Security Section/Department or the function charged with this responsibility/Designated person]** shall permit access to secure areas, and records of that authorization must be kept.
3. Users shall refrain from eating or drinking near information processing facilities and equipment. Food shall be consumed at the designated place allocated by the Entity.
4. Users shall keep electronic media such as DVDs, Flash drives etc., containing confidential information inside the locked cabinets or drawers thus protecting them from attempts of unauthorized access.
5. Users shall refrain from smoking inside the premises of **[Entity Name]** apart from the designated smoking zones.
6. All documents shall be protected in accordance with their classification level and specific protection requirements.

Physical Security Monitoring

1. CCTV cameras shall be deployed at all entry & exit points in addition to areas that contain critical information, and all movements shall be recorded in line with the ADMCC (Abu Dhabi Monitoring and Control Centre) requirements.
2. The CCTV footage shall be maintained for a minimum period of 30 days before recycling.
3. An alarm system shall be installed at all emergencies exits to avoid unauthorized access to the premises.

Late Working/Working on Holidays

1. Accessing the premises for the purpose of working late or during holidays or weekends shall be authorized and maintained in logs.

Movement of Information Assets

1. All incoming/outgoing and movement of information assets (such as servers, desktops, laptops, network devices etc.) shall be recorded by the respective [**Information Technology head/manager or the job title assigned with this responsibility].** Information assets that are sent out for maintenance or repair shall be recorded by the respective **[Information Technology head/manager or the job title assigned with this responsibility]**
2. Retirement of information assets shall be authorized by the respective section manager and approved by the **[Information Technology section/department or the function assigned with responsibilities of Information Technology Management, or the function assigned with assets management].**

Environmental Security

1. Temperature, humidity, and flooding sensors shall be installed and monitored regularly at the Datacenter hosting critical servers, medical devices and networking devices.
2. Appropriate safeguards against environmental and other external threats must be applied to all premises, including but not limited to, data center and office space, to protect employees, sensitive information, and other assets.
3. The entity shall install a Battery backup, also known as an uninterruptible power supply (UPS), at least for CCTV and the other business critical system such as EMR to provide a backup power source in the event of a power outage.

Fire Suppressions System

1. All information processing facilities of **[Entity Name]** shall have adequate protection against agents causing fire by proper installation of preventive controls.
2. Fire extinguishers shall be placed at visible and easily accessible points **at [Entity Name]** premises.
3. Smoke detectors shall be installed throughout the premises.
4. Firefighting systems, fire detection and suppression systems must be tested and maintained by the **[Unit/Department assigned with responsibilities of physical building security].**
5. Fire Drill/Earthquake drills and training will be provided to employees on periodic intervals.

6. Fire Drill records reports shall be maintained with the respective functions, reports will include time taken in evacuations of the building, learnings from the drill.

Cable Security

1. Adequate planning and designing shall be carried out before installation of new or changes to existing communication/networking connectivity within the premises.
2. All electrical installations shall be properly insulated; loose ends cables shall not be connected to live electrical systems.
3. Communication and Network cabling shall follow the standard norms and shall have similar cabling precautions as mentioned in electric cables.
4. Proper earthing shall be carried out throughout the **[Entity Name]** premises.
5. Communication and network equipment, cables shall be installed in places with minimum Electromagnetic Interference and shall be properly insulated.
6. All kinds of cables shall be laid under the ground/floors or enclosed with proper shields or enclosures.
7. Network equipment shall be positioned in permanent locations away from easy reach. Cabling from Network equipment to systems shall be through concealed channels.
8. Network Termination points shall be installed in permanent fixtures.

Protection of Equipment

1. The environmental condition of information processing facilities shall be maintained in accordance to the entity's risk environment or manufacturer recommendations.
2. The assets owners of the information processing facilities shall carry periodic maintenance of the equipment to ensure continuous operational conditions and prevent damage from dust and pollution.
3. The critical equipment purchases shall be supported with adequate vendor support and defined service level agreements.
4. Periodic maintenance shall be conducted of physical security systems such as CCTV, Fire protecting devices, Generator, UPS etc. as applicable and relevant records shall be maintained.

Incident Reporting

1. All incidents related to the physical and environmental security shall be reported to [Information Security Section/Department or the function assigned with information security responsibilities] as per the Entity Information Security Incident Management procedures (that is to be developed by the Entity based on the need)

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure the Code of Conduct for Employees and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

5. Access Control Policy

Objectives

The Access Control Policy defines the controls that need to be implemented and maintained to protect information assets against unauthorized access that poses substantial risk to the entity. The policy

intends to establish adequate controls for user access management, networks access, operating system security and mobile computing in **[Entity Name]**

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, information, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. The **[Information Security Section/Department or the function assigned with information security responsibilities]** shall maintain a list of Users having primary responsibility for information assets/systems/application and the information assets to which their authority extends.
7. **[System Administrators or the job title assigned with responsibilities of systems administration]** are responsible to implement the defined security controls on the respective information systems.

Policy Statement

User Access Provisioning

1. All formal procedure shall be in place for user registration & de-registration.
2. All access privileges shall be allocated on a “need basis” – only the minimum privileges required for the user’s functional role shall be allocated.
3. Access to all systems, applications, medical devices/equipment and services that process, use or store Health Information shall be authorized and authenticated.
4. The inactive sessions shall automatically end after a predetermined interval
5. User access provisioning should be initiated in the following cases, but not limited to:
    a) New employment
    b) Users being promoted/demoted/transferred.
    c) Temporary assignment of job responsibilities
    d) Access to external Users (such as vendors, contractors, and partners) & third parties, etc.
6. All high privilege access shall be provided only after approval **[Information Security Manager or the job title assigned with responsibilities of managing information security]** and **[Assigned person from Top Management].**
7. Change the default admin credentials to a strong, unique username and password that are not easily guessable. If unable to do so, limit the number of people who have access to the administrator account and keep a record of who has access.
8. Any information systems’ service account or shared account shall be created with explicit approval from the Information System Owner, Business Processes Owner & shall have an owner assigned to ensure accountability.
9. The list of service accounts or shared accounts shall be identified & documented by respective systems administrators. The normal user accounts must not be used as service accounts or used to conduct privileged application and system level activities.
10. Shall create service account with non-integrative login with least privilege as applicable.

User Access De-Provisioning or Adjustment

1. User Access de-provisioning is valid under the following circumstances:

a) End of User's service.

b) If requested by the Director/Manager of the concerned department

c) External Users such as (vendors, contractors and partners) & third parties, etc., completing their engagement.

d) Change of function/department within the entity

e) If a User is found to have violated any policy or misused the provided access in any mean.

2. Process shall be defined to ensure that access rights associated with users are revoked upon termination of their employment, contract, or agreement.

3. The **[HR section/department or the function assigned with HR responsibilities]** shall be responsible of initiating the de-provisioning of user access for the resigned or terminated user, in coordination with the respective manager of the user.

4. The **[HR section/department or the function assigned with HR responsibilities in co-ordination with Information Technology Section/department]** shall be responsible of defining procedure for access revocation due to resignation or termination of employees.

5. The **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** shall be responsible of ensuring access revocation of the resigned or terminated user from all information processing facilities which the user had during the tenure of employment with **[Entity Name]**.

6. **The [Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** shall be responsible of verifying and signing the access termination of the resigned or terminated user.

7. The removal or modification of access rights for terminated **[Entity Name]** users shall be carried out by the **[Information Technology Section/Department or the function assigned with responsibilities of Information Technology Management]**

8. On completion of revocation of access, the **[Information Security Manager or the job title assigned with responsibilities of managing information security]** shall review and endorse the access termination evidence.

9. The entity shall retain the records of exit employees with the details of revocation of access.

User Access Authentication

1. Users shall be provided with a unique User ID combined with a password for authentication, as a minimum.
2. Users shall be provided with one ID per system or application with the appropriate privileges mapped to carry out their day-to-day activities.
3. **[System Administrators or the job title assigned with responsibilities of systems administration]** shall assign unique user identification to the authorized user upon notification of access request approval.

Access Related to Third Party (vendors/consultants)

1. All contracts with third party (such as vendors, contractors and partners) & third parties shall include security requirements and clauses outlining the access requirements to **[Entity Name]** systems.
2. The **[Function responsible of contracts management]** and the **[Information Security Manager or the job title assigned with responsibilities of managing information security]** shall review and agree on any special requirements related to providing access to vendors/consultants and ensure including such requirements in the contracts/agreements. **The [Information Security Manager or the job title assigned with responsibilities of managing information security]** reserves the right to require additional access controls to be applied in relation to any contract.

Review of Access

1. The **[System Administrators or the job title assigned with responsibilities of systems administration]** shall generate Users list from the Information Systems and network devices on a regular basis, this list shall be reviewed by Business Owner and the directors/managers of the users, to identify redundant, dormant, or expired user accounts, or incorrect privileges. User accounts that are inactive for a period of <<maximum 90 days>> shall be disabled by [System Administrators or the job title assigned with responsibilities of systems administration] on a regular basis.
2. All privileged, service and administrators accounts shall be reviewed on a quarterly basis, and changes to such accounts shall be logged for periodic review.
3. The entity shall retain user access review records as required.

Network Access Control

1. Provisioning or de-provisioning of access to **[Entity Name]** network & its services shall be carried out in accordance with the Access Control Policy and User access management procedures (to be developed by the Entity based on the business needs).
2. **[Network Administrators or the job title assigned with responsibilities of Network Management]** shall ensure that only authorized Users are able to access network resources.
3. Unwanted ports and services, configured on any network equipment, shall be disabled, or removed.
4. For shared networks, especially those extending across **[Entity Name]**'s boundaries, strict access control shall be implemented to restrict unauthorized access as per business requirements.
5. The configurations of all network and security devices shall be backed up as per the Entity Information-Data Backup Policy.
6. The default passwords of network and security devices shall be changed by the [Network Administrators or the job title assigned with responsibilities of Network Management] immediately after installation.
7. All Passwords of network or security devices shall comply with the Entity Password Policy.
8. Access to all diagnostic ports will be provided after approval from **[Information Technology Section Head or job title assigned with the authority].** Connection to the remote diagnostic ports will be provided using secure communication channels.
9. Every sensitive and high-reliability system managed by or owned by **[Entity Name]** should be protected from outside access using firewalls and relevant controls etc.
10. All network and security devices shall be protected against physical and environmental threats in accordance with the Entity physical and environmental security policy.
11. Failover mechanism shall be deployed when setting up all network devices, to avoid single point of failure that could cause the unavailability of the network services.
12. Segregation, in the form of multiple DMZ's, shall be implemented when publishing public facing services.

13. Change management procedure and proper authorization shall be followed prior to modifying configurations of any network and security device.
14. **[Network Administrators or the job title assigned with responsibilities of Network Management]** shall harden all network devices as per the approved minimum security baseline documents.
15. All Information systems shall be logged out or sessions terminated automatically after a defined period of inactivity.

Remote Access Security

1. Provision of remote access shall be provided based on the need to know and need to use basis and after necessary approval.
2. **[System Administrators or the job title assigned with responsibilities of systems administration]** shall only grant remote access to authorized personnel.
3. Remote access shall be authenticated using a two-factor authentication mechanism.
4. Restrict remote access to entity's systems from outside United Arab Emirates (UAE)

General Guideline on User Access

1. Users shall be held responsible for all activities carried out using their access accounts.
2. Users shall refrain from sharing or declaring any of their access control credentials with anyone.
3. The password of all generic accounts shall be changed immediately by the **[System Administrators or the job title assigned with responsibilities of systems administration]** of the information systems when a User or Users of the account have resigned/terminated or transferred. A record shall be maintained for the change of password respectively.
4. Users shall be aware of their access rights and the terms & conditions for use in the respective information systems.
5. All User access request records shall be maintained for reference & audit process for a period of (to be decided by the Entity based on the risk, business need and any legal or regulatory requirements applicable to the Entity or the specific information).
6. All records related to User access shall be destroyed on completion of the defined retention period.
7. Access to shared folders shall be authorized for business purposes only.

8. Users shall report any kind of misuse or unauthorized access of their access credentials or any other security incidents related to User's access.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees, and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.
5. The **[Information Security Section/Department or the function assigned with information security responsibilities]** in coordination with the Information Systems Owners, Business Processes Owners reserve the right to review Users' lists and ascertain the privileges granted.
6. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to review the use of high privilege IDs at regular intervals.

6. Communications and Operations Security Policy

Objectives

To ensure the appropriate and secure operation of information processing assets and to ensure that communication of **[Entity Name]** information/data shall is managed and controlled with appropriate process and procedures to reduce the risk of inappropriate communication and deliberate system misuse.

Effective Communications and Operations management will have outcome including, but not limited to:

- Improved security and reduce probabilities of compromise.
- Reduced errors
- Controlled unauthorized activities.
- Availability and integrity of the data
- Regulated efforts
- Increased efficiency
- Reduced security incidents

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, information, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. **The [Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.

3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. **[System Administrators or the job title assigned with responsibilities of systems administration]** are responsible to adhere to this policy in their day-to-day activities.
7. **[Information Technology Section/department or the function assigned with responsibilities of IT Management]** is responsible to ensure compliance with this policy.

Policy Statement

1. **[Entity Name]** shall control support and maintenance of information systems concerning data, technology, and application.
2. Implement controls to secure **[Entity Name]** against existing and evolving threats.
3. Controls shall be in place to protect the exchange of information through all types of communication facilities based on the criticality of the data transferred through the channel.
4. **[Entity Name]** shall ensure that all relevant documentation including software details is obtained from manufacturer/vendor/supplier about the information assets, as applicable.
5. Depending on how important the information being sent over the channel is, controls must be put in place to safeguard the transmission of information through all forms of communication facilities.

Capacity Management

1. Critical parameters and their thresholds shall be monitored for all critical infrastructure elements and software(s) at periodic intervals to ensure required performance levels and availability.
2. All sections of **[Information Technology Section/department or the function assigned with responsibilities of IT Management]** shall ensure the availability of adequate capacity of IT resources to deliver the required IT services pertaining to their areas of operations.

3. All sections of **[Information Technology Section/department or the function assigned with responsibilities of IT Management]** shall conduct forecasting reviews to anticipate future needs of IT requirements for delivering the IT services in alignment with the strategic direction of **[Entity Name]** and upcoming projects and initiatives. These capacity requirements shall be documented as IT capacity plans.
4. Capacity planning shall take account of new business and system requirements and current and projected trends in the **[Entity Name]** information processing capabilities.
5. The periodicity of capacity review shall be defined taking into consideration the criticality of the infrastructure element, lead time/costs to procure replacement, and the parameter being monitored.
6. All sections of **[Information Technology Section/department or the function assigned with responsibilities of IT Management]** shall continuously monitor, analyze, and evaluate the performance and capacity of all IT infrastructure and services, to ensure that no excessive systems resources are consumed and there is no significantly degrading systems response time.
7. To ensure the required system performance and to prevent abuse and excessive resource use, computer and network resources will be monitored, tuned, and projections shall be made for future capacity requirements.

Change Management

1. Changes to IT infrastructure shall be carried out in compliance with the [Entity Name] Change Management Procedures (to be developed by the Entity based on the business needs).
2. Changes to all information processing asset will be controlled and documented to ensure that any changes and additions do not compromise information security.
3. Any change to the **[Entity Name]** information processing facilities and systems shall be performed only when there is an approved change request in place.
4. All change requests shall be assessed for possible risks to system, users, business, operations, and infrastructure before its implementation.
5. The change request shall at least include the following:
    - Category of the Change (Emergency/Normal/Standard)

- Affected Services.
- Change Description.
- Reason for Change.
- Business impact of the change.
- Information Security requirements for change implementation.
- Expected date of completion.
- Rollback plan.
- Priority of the change
- Change Advisory Board approval (as applicable); and
- Comments

6. A designated representative or Change Advisory Board (CAB) shall be formed as applicable to manage and authorize change requirements that affect the operational IT Business applications and IT Infrastructure Environment.
7. The Change Advisory Board (CAB) comprises of representatives from:
    - Information Technology Teams (Network, Servers/Systems, End User Support, Security, Application, Help Desk, etc.) – as applicable.
    - Information Security Section/Department
    - Associated Business Function
    - Change Manager
8. Change Request initiated shall be documented and managed.
9. All change requests shall be prioritized, assessed, approved, planned, tested, and implemented in accordance with the procedure defined for Change Management
10. Any change that affects the confidentiality, integrity, or availability of the system, supporting systems/other
11. systems and/or the environments shall be assessed and addressed.

12. All changes shall be tested prior to the deployment in production/operating environment and the evidence shall be retained.
13. All changes must be scheduled, and all the affected parties must be informed in advance of the change.
14. All changes shall be reviewed after the roll out. The change implemented shall be monitored and assessed for any impact on the system, supporting systems and the environments.
15. An appropriate version control document shall be maintained for all the changes made to the applications as well as IT components.
16. All changes shall have a back out/roll-back plan or procedure in place.
17. The entity shall retain the records pertaining to changes.

System Acceptance

1. Before connecting any computer system and/or device to [Entity Name] network, the following checks shall must be performed, at minimum by **[Information Technology section/department or the function assigned with responsibilities of Information Technology Management]**
    - Default admin password change
    - Deployment of latest patches
    - Anti-virus/Anti-malware controls with latest definition
    - Disable unnecessary services.
    - Ensure no factory defaults.
    - UAT testing if applicable.
2. The acceptance and sign-off of **[Information Technology Section/department head/manager or the job title assigned with responsibilities of IT Management]** will be obtained prior to putting any changes, upgrades and releases into production state.

Antivirus and Anti-Malware Controls

1. All sections of **[Information Technology Section/department or the function assigned with responsibilities of IT Management]** shall ensure that Antivirus software is installed on all information systems connected to [Entity Name] corporate network.
2. The entity's IT/designated individual shall implement necessary controls to eliminate stopping of Antivirus services by users from system.
3. The entity shall ensure that the installed Anti-Virus solution (DATs) is updated, and automatic scans are performed periodically.
4. The users shall notify the IT/designated individual in case of any virus/malicious alerts.
5. The Entity's IT shall disconnect the infected system from the network and shall take necessary actions to eradicate the virus/malicious alerts.
6. Virus scan shall be performed to scan any files before they are restored from backup storage media to a production system and prior to connecting any removable media devices such as USBs, External Hard Disk drive etc.
7. Entity shall implement relevant controls to refrain end users from browsing malicious web sites, downloading malicious contents/software.
8. All Information assets/technology/medical devices/ equipment shall be updated timely without fail.

Backup Management

1. Backup requirements shall be identified for all information assets connected to **[Entity Name]**'s corporate network.
2. Backup of information/data shall be performed as per the backup and archival requirements identified by the respective information/Information assets Owners.
3. A formal backup plan shall be documented identifying the information systems, information to be backed up, type, frequency (Daily/Weekly/Monthly etc.) and retention of backups.
4. Entity shall ensure that the identified backup requirements are aligned with the RPO (Recovery Point Objective) of Business Continuity Plan of Entity as applicable.

5. Information/asset owners shall provide the application specific backup requirements or data backup requirement to the Information Technology Section/department as and when required.
6. Entity shall clearly define the scope and responsibilities of backup such as who owns the process, where the backed-up data has to be stored, retention requirements etc. in the contract with clear SLAs if the backup process is handled by Vendors/Third parties such as EMR vendors and outsourced IT etc.
7. Entity shall not store/maintain/keep backed up data in the same system where the backup is being taken.
8. Backup results shall be recorded. In case the backup fails, root cause analysis shall be performed and necessary actions to be taken to re-run the backups.
9. Entity shall implement appropriate Physical and Logical access controls to protect the media that contains backup.
10. Entity shall define an approval process prior to the movement any media that contains backups such as moving a media from onsite to offsite etc.
11. Entity shall ensure that the periodic restoration tests are conducted, results are recorded and retained.

Logging and Monitoring

1. All significant security-relevant events, such as password guessing attempts, user activity, security events, attempts to use privileges that are not authorized, modifications to production application software, and system software, login attempts etc. will be securely recorded for Information assets and technologies handling sensitive, valuable, or critical information.
2. **[Information Security Section/Department or the function assigned with information security responsibilities]** will decide the Log retention period of an asset basis of asset value. This list would be reviewed once every year.

Clock Synchronization

1. All systems clocks along with the clocks in medical devices and equipment shall be synchronized using Network Time Protocol (NTP) to ensure the accuracy of audit logs.

2. Users shall be restricted from changing the system's time.

Security Assessment and Vulnerability Management

1. Timely information about technical vulnerabilities in infrastructure elements and software(s) being used shall be obtained from trusted sources (e.g., through subscription to vendor security advisories). Vulnerability Assessments and Penetration Tests shall be conducted periodically.
2. **[Information Security section/Department or the function assigned with information security]** is responsible for conducting periodic vulnerability assessments and penetration tests on the Information Technology management.
3. **[Information Technology section/department or the function assigned with responsibilities of Information Technology Management]** shall facilitate the **[Information Security Section/Department or the function assigned with information security]** efforts when conducting a vulnerability assessment or a penetration testing exercise.
4. Timelines shall be defined for responding to identified/reported technical vulnerabilities.
5. **[Information Technology section/department or the function assigned with responsibilities of Information Technology Management]** shall address the vulnerabilities identified through the security assessments in coordination with **[Information Security Section/department or the function assigned information security responsibilities]**
6. Information obtained regarding vulnerability shall be evaluated to assess risk to **[Entity Name]** infrastructure. The evaluation shall take into consideration:
    - Vendor reported criticality (e.g., high, medium, and low)
    - Likelihood of the vulnerability being exploited (e.g., existence of a known exploit or other malicious code that uses the vulnerability as an attack vector)
    - System criticality (e.g., the relative importance of the applications and data the system supports at **[Entity Name]**; and
    - System exposure (e.g., proxy server vs. internal file server vs. application servers)
7. The identified risk shall be categorized as per the severity of the risk.

8. The vulnerability must be addressed with the proper procedures. If the vulnerability cannot be fixed, compensating controls must be implemented to lessen the risk's impact.
9. A revalidation scan shall be performed to ensure that the vulnerability has been fixed after the patch or solution for high-risk vulnerabilities has been applied.
10. **[Information Technology Section/department or the function assigned with responsibilities of Information Technology Management]** shall have minimum security baseline (hardening) documents for all critical IT information systems such as servers operating systems, applications, databases, network, and security devices etc.,
11. The security baseline documents shall be updated periodically to address the latest vulnerabilities.
12. The **[Information Security Section/Department or the function assigned with information security responsibilities]** shall review and sign-off on the baseline documents.
13. **[System Administrators or the job title assigned with responsibilities of systems administration]** shall implement the applicable security baseline documents on all IT information systems prior to deployment.
14. **[System Administrators or the job title assigned with responsibilities of systems administration]** shall also ensure that the information systems under their responsibility conform to these baselines requirements on an ongoing basis.

Patch Management

1. **[Entity Name]** shall develop a procedure that ensures all system components connected directly or indirectly to the **[Entity Name]** environment have proper and required patches installed timely.
2. **[Information Technology Section/department or the function assigned with responsibilities of Information technology Management]** shall ensure that all information systems have the latest stable security patches installed to mitigate the risks associated with vulnerabilities that may exist in the currently installed versions. This includes all servers, desktops, laptops, applications, databases, medical devices, network devices, security devices and other IT systems etc. The patch information shall be obtained from the following sources:
    a) Patches released for OS Platforms and Networking components from the respective vendors.
    b) Vendor websites for security patches

3. Prior to deployment of patches in information systems, patches shall be validated and tested including security patches and system upgrade patches.
4. **[System Administrators or the job title assigned with responsibilities of systems administration]** shall adhere to the Change Management Process, schedule proper downtime for deploying patches and ensure that a roll-back plan is identified before deploying any patch.
5. Timelines for patch implementation shall be defined and agreed with the respective information Systems Owners and business owners.
6. **[System Administrators or the job title assigned with responsibilities of systems administration]** shall keep record of the current level of patches deployed with respect to the information systems. The patch management shall be performed in compliance with the Entity Patch Management Procedures (to be developed by the Entity based on the business needs).
7. Analyze the results of patch deployment over the patch management tool and identify the list of missing patches on the desktops/Laptops and servers.
8. Initiate the action plan for deployment of missing patches.
9. **[Information Security Section/Department or the function assigned with information security responsibilities]** would co-ordinate with the [System and Network Administrators or the job title assigned with responsibilities of systems and Network administration] to resolve the discrepancy and would direct to apply the patches after the discrepancy is resolved.
10. **[System and Network Administrators or the job title assigned with responsibilities of systems and Network administration]** must monitor the status of patch or service pack or update installation on the systems or devices.
11. **[System and Network Administrators or the job title assigned with responsibilities of systems and Network administration]** must maintain the list of servers and networking devices with updated patches or upgrades to keep track of patch implementation.

Electronic Communications Security

Electronic Communication Services Access Provisioning & De-Provisioning

1. Electronic communication accounts shall be created as per the Entity approved process.

2. Any generic or group email account shall have an owner assigned for accountability.
3. Electronic communication accounts de-provisioning (disabling) request shall be raised per [Entity Name] approved process.
4. Electronic communication accounts de-provisioning (disabling) is valid under the following circumstances:
    - End of employee's service.
    - Contractors completing their engagement.
    - If requested by the Director of the concerned department to which the user belongs.
    - If user found to have violated the policy or misused the provided service in any mean.

General Guidelines for Communications Security

1. All electronic communication resources provided by **[Entity Name]** shall be used for official purpose only.
2. Users shall refrain from using the official electronic communication resources for personal communications/correspondences.
3. All official electronic communication correspondences, unless otherwise specified, shall be treated as **[The Entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.].**
4. All electronic communication correspondences must be properly addressed to the intended recipient.
5. All Users shall be held responsible for any misuse of electronic communication correspondences from their accounts, if proven to be an intentional act from the User.
6. Users shall refrain from initiating or participating in any electronic communication or newsletters not related to the job duties, such as forwarding chain emails whether commercial or with personal amusement and entertainment content.
7. Using email to send or forward large attachments containing graphics/objects/video files that can result in disruption of email services is prohibited.

8. Users shall make use of authorized file sharing tools, such as file servers or document management tools, provided by **[Entity Name]** to share huge official attachments.
9. Users shall refrain from sending information, software, files or attachments that are illegal or unauthorized, or include any defamatory, offensive, racist or obscene remarks.
10. Users shall refrain from accessing or using any electronic communication account of other Users, unless it is authorized/delegated by the account owner with proper business justification, and this shall be requested from and processed formally by the responsible unit in **[Entity Name]** and without sharing the password of the account.
11. Users shall refrain from using personal emails for official communications/correspondences.
12. Users shall be responsible for the protection of any local copy of mailboxes stored in their laptop or desktop.
13. Users shall be responsible to archive their emails as per the **[Entity Name]** approved archival procedure.
14. Users shall promptly report any kind of security incidents on the electronic communication resources as per the **[Entity Name]** Information Security Incident Management process) that is to be developed by the Entity based on the need).
15. Users shall refrain from sending email attachments that may spread viruses (such as .exe, .bat, .com, .scr, .vbs, .jar etc.).
16. Users shall refrain from configuring automatic forwarding of official emails to non-**[Entity Name]** hosted email system.
17. Security risks associated with the exchange of information in any format, such as email, file transfers, mobile devices, etc., with external entities shall be prevented by the implementation of suitable security controls.

Information Exchange Agreements

1. Contracts/Agreements must be made for the manual or electronic sharing of **[Entity Name]** information and other information assets with third parties.

2. Prior to signing the contract, **[Entity Name]** shall verify that external parties are aware of the information security needs and policies that are necessary.
3. Exchange agreements shall have an expiration date and be periodically reviewed to ensure ongoing business necessity.
4. Information Exchange agreements shall consider the following security conditions, as required:
    a) management responsibilities for controlling and notifying transmission, dispatch, and receipt.
    b) procedures for notifying sender of transmission, dispatch, and receipt.
    c) procedures to ensure traceability and non-repudiation.
    d) minimum technical standards for packaging and transmission
    e) responsibilities and liabilities in the event of information security incidents, such as loss of data
    f) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood, and that the information is appropriately protected.
    g) ownership and responsibilities for data protection, copyright, software license compliance and similar considerations
    h) technical standards for recording and reading information and software.
    i) any special controls that may be required to protect sensitive items, such as cryptographic keys.

Physical Media in Transit

1. Entity shall define an approval process for Media movement.
2. **[Entity Name]** shall define labelling requirements for physical media carrying sensitive information.
3. **[Entity Name]** shall identify measures to be taken in the event of loss of physical media in transit.
4. **[Entity Name]** shall maintain records of all media movements.

Network Security Management

1. **[Networking section or the function assigned with responsibilities of network management]** shall design **[Entity Name]** communications networks so that no single point of failure could cause network services to be unavailable.

2. **[Networking section or the function assigned with responsibilities of network management]** shall maintain up-to-date network documentation includes up to date network architecture diagrams and configuration files of devices (e.g., routers, switches)
3. All unused connections and network segments will be disconnected from active networks (Ports and ACL rules etc.)
4. Permission to connect third party computers (Third Party/Consultant/Auditor) would be given on the approval of **[Information Technology Section/department Head/manager and the Information Security section/department Head/manager].**
5. All web servers accessible through the Internet shall be protected by a firewall as required. All connections between **[Entity Name]** internal networks and the Internet or any other publicly-accessible computer network shall include an approved firewall and related access control system.
6. Changes to Firewall configuration rules will only be made on explicit permission of **[Information Technology Section/department Head/manager or the job title assigned with responsibilities of Information Technology Management].**
7. Appropriate logical segregation shall be done through creation of zones such as VPNs.
8. Periodic configuration backups of network devices such as Firewall shall be taken by the **[Entity Name]**

Wireless Security

1. The management and maintenance of Wireless Infrastructure shall be carried out by the **[Networking section or the function assigned with responsibilities of network management].**
2. The **[Networking section or the function assigned with responsibilities of network management]** shall be responsible for ensuring wireless access points are configured to use strong authentication and cryptographic methods.
3. Corporate wireless networks shall be segregated from guest wireless networks.

Information Systems Security

1. All default accounts of information systems shall be renamed (where possible) and the default passwords shall be changed.

2. **[System Administrators or the job title assigned with responsibilities of systems administration]** shall have unique administration accounts separate from the normal accounts that are used for activities not related to systems administration.
3. Minimum and only required administrative privileges shall be assigned to admin accounts to carry out the required administrative tasks.
4. Passwords of all High privilege accounts such as administrator, root etc. shall be set with at least 10 characters and complexity as per the Entity Password Policy.
5. **[Information Security Manager or the job title assigned with responsibilities of managing information security]** shall be responsible to verify the usage of information systems high privilege accounts once every three months.
6. **[System Administrators or the job title assigned with responsibilities of systems administration]** shall not change privileges to any account without proper authorization and approvals as per the Entity Access Control Policy.
7. Any change in the configuration of information systems shall be done as per the Entity change management procedure (to be developed by the Entity based on the business needs) where proper approval is obtained.
8. **[System Administrators or the job title assigned with responsibilities of systems administration]** of Domain controllers shall not change, create, or delete group policies without getting proper authorization and approvals.
9. **[System Administrators or the job title assigned with responsibilities of systems administration]** shall harden the information systems as per the approved minimum security baseline requirements (to be developed by the Entity based on the business needs).

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees, and any other applicable UAE Laws in this regard.

2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from [Information Security Head/Manager or the job title assigned with responsibilities of information security] on a case-to-case basis.

7. Data Privacy Policy

Objectives

The objective of the data privacy policy is to establish clear guidelines and responsibilities for **[Entity Name]** and its staff in safeguarding Personally Identifiable Information (PII) and Protected Health Information (PHI). The aim of this policy is to ensure the confidentiality, integrity of patient data to protect against unauthorized access, disclosure, or misuse.

Scope

This policy applies to all users and all operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media used to store, process, transfer and manage PII and PHI Health Information

Responsibilities

1. The **[Information Security Manager/Data Protection Officer or the job title assigned with responsibilities of managing /Data Privacy]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with Data Privacy responsibilities]** is responsible to assist the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with Data Privacy]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. The **[Director or job title assigned with responsibilities of Entity's higher management]** of **[Entity Name]** shall endorse this policy for its effective implementation.

Policy Statement

Protected Health Information Privacy and Protection

1. The **[Entity Name]** is committed in protecting the security and confidentiality of the personal information processed from Data Subjects including, but not limited to, employees, patients, customers, business partners, vendors, third parties, service providers, suppliers, former employees, and job applicants.
2. The **[Entity Name]** is aware of the importance of effectively safeguarding and responsibly managing PII and PHI
3. The **[Entity Name]** adheres to the following privacy principles to ensure your data is processed in an appropriate and safe manner.
4. **[Entity Name]** respects the privacy of all [Data Subjects] including but not limited to, employees, patients/customers, business partners, vendors, third parties, service providers, suppliers, former workers, and job applicants, and is aware of the importance of protecting and managing Protected Health Information appropriately.

Consent Collection

1. **Choice and Consent:** The **[Entity Name]** shall obtain explicit consent from the **[Data Subject]** before the collection of their PII and PHI. The consent shall include the right of the **[Data Subject]** to withdraw from it.
2. The Entity shall keep records of the consent taken from the **[Data Subject]** to demonstrate compliance.

Fair, Legitimate and Transparent Processing

1. The **[Entity Name]** will process PII and PHI of the [Data Subject] in a fair and lawful manner.
2. The **[Entity Name]** will provide the [**Data Subject**] with a clear description of the purpose their PII and PHI has been collected for and a detailed version of the information will be made available to the [**Data Subject**] through the consent form and the **[Entity Name]**'s Privacy Policy. The **[Entity Name]** will adapt to a general policy of transparency about developments, practices, and policies with respect to the PII and PHI

Collection Limitation

1. The **[Entity Name]** will collect PII and PHI of the **[Data Subject]** limited to the purposes identified in the consent furthermore, any such information shall be obtained by lawful and fair means, and where appropriate, with consent of, the patient/customer or associate concerned.
2. Additionally, the **[Entity Name]** will follow the principle of data minimization and will collect limited and relevant PII and PHI in relation to the purpose for which they are processed.

Use Limitation

1. PII and PHI of **[Data Subject]** will not be made available or otherwise used for any purpose other than what was agreed with that individual at the time of data collection.

Access

1. **[Data Subject]** will be given access to his/ her PII and PHI that the entity has gathered or stored in its systems, and he/she will be provided with an opportunity to correct his/her PII and PHI thereby assuring that their PII and PHI is accurate**. [Entity Name]** will erase, rectify, complete, or amend the PII and PHI to a justified request.
2. [Data Subject] may request **[Entity Name]** to review, correct, update, suppress, or otherwise modify any of PII and PHI. The **[Data Subject]** may object PII and PHI processing and the decisions made by automated processing.
3. All such requests will be routed through the Data Protection Officer or equivalent.
4. The **[Information Security Manager/Data Protection Officer or the job title assigned with responsibilities of managing Data Privacy]** in consultation with the respective Section/Department should support the closure of the request and ensure providing the data in a machine-readable format. However, **[Data Subject]** will be informed in priority if the request:
    a) The request is not relevant to its own PII and PHI or is excessively repetitive.
    b) The request is inconsistent with the judicial procedures or investigations conducted by the competent authorities.
    c) The request may negatively affect the efforts of the controller to protect information security.
    d) The request violates the privacy and confidentiality of others' personal data.

Security

1. The **[Entity Name]** will protect PII and PHI that it handles, with appropriate technical and organizational safeguards for security, against threats (internal and external security threats), such as loss of confidentiality, integrity, unauthorized destruction, usage, or other misuses. To protect against the risk that PII and PHI may be compromised by internal and external security threats, the entity relies on information protection controls:
    a) **System controls:** User access measures, Network security, Data security etc.
    b) **Process controls:** data classification policies, data backup and retention policy, compliance audits etc.
    c) **People controls:** Signing of NDAs and/or DPAs, training, awareness, employee background checks, and/or any other project specific requirements.
2. The **[Entity Name]** will ensure that PII and PHI or its backup in any form is not stored, processed or transferred outside UAE, except in cases where a valid exemption to do so is issued by DoH is in place.

Disclosure to Third Party/Data Processors

1. The organization will disclose PII and PHI of a **[Data Subject]** to a third party only with the explicit consent of the **[Data Subject].** For every new engagement with a third party or renewal of existing engagement where the PII and PHI is disclosed to third party, the following must be ensured:
    a) To evaluate risk exposure of all third parties
    b) Initial due diligence to be conducted.
    c) Include privacy and data protection provisions in the Contract/Service Level Agreement

Accuracy

1. The **[Entity Name]** will keep the PII and PHI as accurate, complete, and up-to date.

Retention and Disposal

1. **[Entity Name]** will retain PII and PHI only for the duration required to fulfill the stated purpose. The **[Entity Name]** may require keeping PII and PHI for a longer period to comply with legal obligations, complaints, and enforce agreements. However, where PII and PHI is no longer needed, the **[Entity Name]** will anonymize the data using identity concealment mechanism.

Cross Border Data Transfer

1. When conducting business, working on **[Entity Name]** projects, or implementing new processes or systems, **[Entity Name]** may require the transfer of PII and PHI to other **[Entity Name]** entities or third parties that are located outside of the **[Entity Name]**'s country of business. **[Entity Name]** can transfer and share PII and PHI in line with adherence to federal and local mandates on data transfer/processing/storage.

Privacy Data Breach Management

1. Privacy breach management establishes requirements for monitoring and responding to PII and PHI potential privacy breaches.
2. The **[Entity Name]** establishes requirements for monitoring and responding to PII and PHI potential privacy incidents in accordance with policy requirements. Privacy incident management shall ensure:
    a) All the privacy incidents shall be reported to **[Information Security Manager/Data Protection Officer or the job title assigned with responsibilities of managing information security/Data Privacy]** through mail ID (Mode to be decided and developed by the Entity).
    b) All privacy incidents shall be recorded and tracked.
    c) Notify DOH - Abu Dhabi Health SOC about breach at the entity and/or the relevant third party/data processor within defined timeline.
    d) Inform the affected **[Data Subject]** about the breach including the level of impact/damage and the measures undertaken for correction and prevention.

Data Processing Inventory

1. The [Entity Name] will prepare Data Processing Inventory to visualize, track, and analyze, how PII and PHI is created, collected, used, shared, and disposed across the entity.
2. The Data processing Inventory will assist in entity Information security and Privacy risk management strategy by streamlining the data collection process and making it transparent.
3. The inventory will include fields including but not limited to.
    - Description of the categories of PII and PHI
    - Details about the data subject

- Individuals authorized to access personal healthcare.
- Period, purpose, limitation, and scope
- Details about data exchange/transfer
- Mechanism of transfer, deletion, modifying or processing
- Data related to the cross-border movement if any.
- Technical and organizational measures related to information security and processing operations.
- Data Flow Diagrams

Data Privacy Impact Assessment

1. Data Privacy Impact Assessments (DPIA) have become an essential components of an effective data privacy program. **[Entity Name]** will conduct DPIA for the privacy related risks in early stages of a project, before the beginning of processing, and run alongside the planning and development process.
2. DPIA will at least contain:
3. A systematic description of the processing operations and the purposes of the processing
4. An assessment of the necessity and proportionality of the processing operations in relation to the purposes
5. The controls to address the risks, security measures and mechanisms to ensure the protection of PII and PHI
6. The **[Information Security Manager/Data Protection Officer or the job title assigned with responsibilities of managing Data Privacy]** will co-ordinate with the relevant support functions and delivery projects to ensure DPIA is conducted as per the defined methodology.
7. **[Entity Name]** will prepare a list of the type of processing operations that are not obligatory to assess the impact PII and PHI and make it available to the public through its website.

Communication and Training

1. **[Entity Name]** will ensure adequate awareness pertaining to data privacy, its importance, and implications, through a targeted and relevant training program to all its patients/customers,

business partners, vendors, third parties, service providers, as required, to reduce the risk of a privacy breach.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees, and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security/Data Privacy responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security /Data Privacy responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager/Data Protection Officer or the job title assigned with responsibilities of managing information security/Data Privacy]** on a case-to-case basis.

8. Cloud Security Policy

Objectives

To safeguard confidentiality, integrity and availability of all IT applications, data, systems, and network resources implemented in a cloud environment and ensure cloud services are acquired, used, managed, and terminated in conformity with all applicable laws and regulations.

Scope

This policy applies to all users, information technology systems, software, databases, applications and network resources that are implemented in cloud and/or managed service infrastructures needed by the **[Entity Name]** for its operations.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. All relevant users are responsible to read, understand and adhere to this policy in their day-to-day activities.
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to relevant Users.
4. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
5. Projects Owners/Projects Managers are responsible for ensuring compliance to this policy.

Policy Statement

1. Use of cloud computing services for work purposes must be formally authorized by the **[Entity Top Management or equivalent].** Authorization shall be given based on proper assessment of the business case and considerations to information security risks associated with cloud computing.
2. The **[Entity Top Management or equivalent]** will certify that security, privacy, and all other IT management requirements are adequately addressed by the Cloud Service Provider (CSP).

3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** shall decide what data may or may not be stored in the Cloud.
4. Classification of data to be hosted on Cloud shall be based on classification scheme adopted at **[Entity Name]**
5. **[Entity Name]** shall ensure that Cloud Service Provider (CSP) has no ownership rights on the data regardless of the format or storage medium
6. **[Entity Name]** shall ensure:
    a) Appropriate Security Control measures shall be implemented by Cloud Service Provider/Application Service Provider/Any Third-Party/Company for guarding against Data leakage/Data corruption/Security breach etc. as well as control measures in place to prevent, detect and react to breaches including data leakage
    b) Due diligence process is followed for selecting a suitable Cloud Service Provider
    c) Cloud environment is physically hosted within UAE including any of the environments, infrastructures, or systems used for backup and disaster recovery
        - Health Information stored in cloud is not extended for access, use or support by
        - Any other entity/party in a multi-tenant environment
        - Any entity/party that provides analytical services
        - any entity/party that provides remote support from outside UAE, except in cases where an exemption to do so is issued by DoH

Service Level Agreement

1. An appropriate service level agreement with the service provider shall be in place to address but not limited to the following:
    a) Sustainability, support for fail safe operations
    b) Security controls for confidentiality, integrity, availability and privacy of the data collected, processed, stored and disposed through cloud services

c) Security control measures to prevent, detect and react to breaches including data leakage and demonstration of the same.

d) Unilateral contract termination/exit clause and Transition support required.

e) Right to Audit or to access information/log by **[Entity Name]** or any applicable law enforcement agencies.

2. Contracts with service provider shall include but not limited to following in addition to the other contractual requirement:

- Service Level Agreement (SLA)
- Data Processing Agreement (DPA)
- Compliance to applicable laws & regulations
- Data ownership
- Data Privacy controls
- Authentication controls
- Log retrievals
- Patch Management
- Configuration Management
- Application/System Security Testing
- Data Recovery plan
- Data Deletion at separation or expiry of contract

Cloud Access Control

1. Appropriate Access control mechanism shall be implemented with reliable authentication mechanism to ensure:

a) Data is not shared accidentally with other customers on the cloud.

b) Cloud service provider/Application service provider/any third-party personnel controls are in place to provide a logical segregation of duties.

c) Logging and monitoring of privilege access shall be carried out.

d) Access review shall be carried out on a periodic basis.

Cloud Data Security

1. Controls related to Operations Security shall be implemented for ensuring Secure Configuration, Application, OS, DB, Web Server, Back-up & Recovery, Change Management, Capacity & Demand Management, Protection against Malicious Code and Monitoring, Auditing & Logging security requirements on cloud.
2. Encryption techniques shall be implemented for cloud data hosting like Data in transit and Data at rest and encryption keys must be secured as applicable.
3. Security standard protocols i.e., HTTPS, VPN, SFTP, TLS etc. shall be considered for data in motion.
4. Non-disclosure agreement to be signed between **[Entity Name]** and the cloud service provider, in compliance to the Third-Party Security Policy.
5. Incident Management to be carried out by the Cloud Service Provider in line with the **[Entity Name]** incident management procedure
6. Applications shall be subjected to vulnerability scanning & findings of known vulnerabilities shall be mitigated
7. Coordinate with cloud service provider on patching application, database & operating system vulnerabilities. Insist if any patches are missed or not updated
8. All access to data, including administrative access, should be logged and routinely audited
9. The migrated application needs to support high availability to ensure 24/7 services for **[Entity Name]**, based on the business requirements.
10. Appropriate business continuity (BC) and disaster recovery (DR) plans needs to be adopted to ensure minimal downtime and meet SLA guarantees.
11. The backup data should be secured using robust encryption techniques, much as operational data
12. Any changes/release to the cloud environment shall be documented, tested and approved prior to implementation.

Exit Process

1. Proper transition and exit management provisions shall be considered to ensure correct procedures (shall be available with CSP) for handing over cloud services back to [Entity Name] or any other CSP.
2. Projects managers/Projects owners shall ensure that proper transfer of knowledge is obtained from the CSP for the operation/maintenance/ withdrawal.
3. Upon completion/termination of an engagement with CSP, the Projects managers/Designated individual shall inform the relevant information assets owners/custodians to revoke the access rights of the CSP that was granted to the cloud services.
4. Secure disposal procedures shall be established, implemented and complete removal of data from all storage media, ensuring data is not recoverable.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees, and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from [Information Security Section/Department or the function assigned with information security responsibilities].
3. The [Information Security Section/Department or the function assigned with information security responsibilities] reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from [Information Security Manager or the job title assigned with responsibilities of managing information security] on a case-to-case basis.

9. Third Party Security Policy

Objectives

To ensure third party services are controlled through suitable procedural obligations and contractual terms to secure privacy and protect information assets. To establish a suitable framework for third party management and define a control environment that shall:

a) Reduce probabilities of information leakage and loss

b) Secure information assets

c) Minimize unauthorized access and usage.

d) Uphold **[Entity Name]** and governmental reputation.

e) Ensure service continuity

Scope

This policy applies to all Users of **[Entity Name]** and it covers all kinds of operating facilities, Information Technology (IT) resources, information, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media that are accessed, communicated to, or operated by Third Parties.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.

5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. Projects Owners/Projects Managers are responsible for ensuring compliance to this policy.

Policy Statement

Note: All contractual agreements with Third Parties shall be in compliance with the regulations the Entity follows in this context. The implementation of this policy shall be in alignment with the laws or regulations applicable to the Entity.

Third Parties Selection

1. The Project Managers/Projects Owners shall follow the Entity tendering and procurement process.
2. Due diligence shall be exercised while evaluating Third Parties services to ensure accuracy of their claimed qualifications and successful delivery of contractual obligations.
3. Project Managers in coordination with Project Owner shall ensure that contractual agreements in terms of legal, business and technical requirements are negotiated and agreed with the Third Parties, before commencing the project.

Non-Disclosure Agreement Sign off

1. The **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections],** Project Managers/Projects Owners and Users in general shall ensure that NDA (Non-Disclosure Agreement) is signed by any Third Party, whenever there is a need to exchange information classified as **[The Entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.]** of Entity Name], whether for contractual purposes or any other justified business need.
2. The **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections],** Project Managers/Projects Owners and Users in general shall make use of the officially approved template of Non- Disclosure Agreement for **[Entity Name]**.
3. The NDA shall be signed by the User/Project Manager and/or **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** disclosing information classified as **[The Entity shall specify the classification level of information affected by**

this control, for example confidential information or internal information or secret, etc.] of **[Entity Name]**'s, and the third party who presents the need-to-know for the disclosed information.

4. The NDA shall be signed before commencing the information disclosure to the third party, whether it is for a project scoping phase or for any other justified business need.

Third Parties Contracts

1. Based on the criticality of the project and the engagement nature, the below clauses can be considered as part of Third Parties contracts:
    a) Clear definition of supplier/vendor responsibilities
    b) Description of product/service being provided
    c) Compliance with legal and regulatory requirements.
    d) Compliance with Intellectual property rights requirements.
    e) Compliance with entity information security policies and procedures and/or any additional security controls, as required
    f) Clear allocation of responsibilities to all the involved parties.
    g) Statement on Non – Disclosure of information.
    h) **[Entity Name]**'s rights to review and audit the compliance with the contracts.
    i) Adequate Service Level Agreements (SLA), where applicable.
    j) Adequate Data Processing Agreement (DPA). where applicable.
    k) Termination clauses and transition support required from the third-party during entity decision to exit agreement and/or use another service/solution
    l) Backup, Service continuity and availability requirements
    m) Arrangements for reporting, notifying and investigating information security incidents
    n) Restricting access to sensitive information
    o) Requirements for involvement of the third party with subcontractors, and the security controls these subcontractors need to implement

p) Change management clauses in the event of changes to scope/services and provisions in the contract/agreement

Right to audit

Identification of Risks related to Third Parties

1. The **[Information Security Section/Department or the function assigned with information security responsibilities]** shall ensure that the periodic information security risk assessment identifies potential Third Parties risks that could compromise the Confidentiality, Integrity & Availability of Information & information processing facilities.
2. Project Manager in coordination with **[Information Security Section/Department or the function assigned with information security responsibilities]** shall identify any additional information security risk specific to the project.
3. The analysis of risks related to Third Parties access to information and information processing facilities shall consider the following:
   a) Possible impacts to the controls of the information processing facilities.
   b) The classification of the information assets;
   c) Processes for identifying, authenticating, authorizing and reviewing access rights of the Third Parties; and
   d) Security controls are in place to control storing, processing, communicating, sharing or exchanging information.
4. All risks identified shall be appropriately addressed through risks mitigation measures.
5. The changes to any third-party scope/activities and provisions in the agreement shall be done through a formal change management process to ensure changes are carefully planned, communicated, and executed in a controlled and systematic manner and in compliance with **[Entity Name]** Information Security Requirements.

Third Parties Access Management

1. The Third Parties shall be provided access to information & information processing facilities as per the Entity Access Control Policy.

2. The Third Parties shall be provided access to information & information processing facilities on the principles of need-to-know basis.
3. The provisioning of Third Parties access to information & information processing facilities shall be granted on temporary basis. Wherever feasible, this access shall be configured with specific end date so that it gets expired at the end of the contract.
4. The usage of non-**[Entity Name]** managed laptops by the Third Parties shall be based on approval from **[Technical Support Section or the function assigned with technical support],** after being authorized by the respective senior management and having proper business justifications.
5. Third Parties shall not be granted remote access before obtaining prior approval as per the **[Entity Name]** Remote Access Policy. Entity shall prohibit access to any of the entity's information processing systems outside UAE unless an exemption approval is obtained from DoH.

Monitoring and Review of Third Parties Services

1. Respective Projects Managers shall maintain appropriate reports and records, to monitor and measure the compliance with the information security requirements. The Third Parties shall be responsible to take appropriate actions to address any non-conformities might be identified during the compliance review.
2. Security events logging shall be fully activated for all information processing facilities to which access is provided to Third Parties as per the contractual obligations.

Termination of Third Parties Services

1. Proper transition and exit management provisions shall be considered to ensure correct procedures for handing over third contracts or services back to the **[Entity Name].**
2. Projects Managers/Projects Owners shall ensure that proper transfer of knowledge is obtained from the Third Parties for the ongoing operation/maintenance.
3. Upon completion/termination of an engagement with Third Parties, the Projects Managers shall inform the relevant information assets owners/custodians to revoke the access rights of the Third Parties that was granted to information processing facilities.

4. Projects Managers/Projects Owners shall ensure that all **[Entity Name]** assets provided to the Third Parties are returned such as laptops, books, manuals, documentation, building keys, magnetic access cards etc.
5. Any connections between the Third Parties' network and **[Entity Name]** corporate network shall be terminated in cases of any security breach that may occur or non-compliance of the Third parties to any of the Entity's policies.

Reporting Information Security Incidents

1. Projects Managers/Projects Owners and all Users of **[Entity Name]** shall report any incidents related to Third Parties to the **[Information Security Section/Department or the function assigned with information security responsibilities]** as per the Information Security Incident Management process (to be developed by the Entity based on the need).
2. **[Entity Point of Contact or the employee assigned with Information Security Incident Communication responsibility]** shall report DoH within defined timelines, in the event of any information security incident in the services provided by third party.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees, and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

10. Information Systems Acquisition Development, & Maintenance Security Policy

Objectives

To emphasis the need for entities to adopt secure system and software development lifecycle management processes and to ensure security requirements are identified and integrated during the acquisition, development and maintenance of applications, software, products and/or services.

Scope

This policy applies to all Users and third-party personnel of **[Entity Name]** involved in the Acquisition, Development and Maintenance of Information Systems and Applications, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. Projects Owners/Projects Managers are responsible for ensuring compliance to this policy.

Policy Statement

Security Requirement of Information Systems and Applications

1. All Information systems acquired and developed shall be aligned with the business requirements and shall be supported by the relevant documentation, approved by the respective Business owner.
2. All Information System and Application acquisition initiatives shall be documented and approvals from Head of the sections shall be obtained.
3. Before a new system is developed or acquired, **[Entity Section/Department]** shall clearly specify the relevant security requirements and inform users and operators of their roles and responsibilities to allocate suitable privileges.
4. Business requirements for new systems or significant enhancements to existing systems will specify the required security controls.
5. All statements of business requirements for new information systems or enhancements to existing information systems shall specify control and system security requirements. It is the responsibility of the Head of the business section who develops the statements of business requirements to identify these security requirements with the help of **[Information Security Section/Department or the function assigned with information security responsibilities]**
6. Security requirements shall include:
    a) Secure coding.
    b) User authentication.
    c) Access provisioning and authorization processes, for business users as well as for privileged or technical users;
    d) Informing users and operators of their duties and responsibilities;
    e) Protecting Information Assets as per the Information Classification and Handling Policy;
    f) Business processes specifics, such as event logging and monitoring, non-repudiation required;
    g) Mandatory security controls, e.g., interfaces to logging and monitoring or data leakage detection system.

7. All software developed in-house that runs on production systems shall be developed according to the Software Development Lifecycle (SDLC).
8. Software shall be adequately documented and tested before it is used for critical **[Entity Name]** information.
9. There shall be a segregation between the production, development, and test environments.
10. Access Controls shall be enforced for production, development, and test environments
11. Testing of production software must always be done using sanitized data and not with PII and PHI or Sensitive information
12. Applications developed shall go through necessary information security testing and approval from **[Information Security Section/Department or the function assigned with information security responsibilities]** shall be attainted before being deployed in production.
13. Entity shall ensure that the vulnerability assessment is conducted and identified vulnerabilities are addressed prior to introduce the developed software into the Entity's environment.

Securing application services on public networks

Adequate security controls shall be put in place to ensure the confidentiality, integrity and availability of the information contained in the publicly available systems of **[Entity Name].** In order to maintain security of application services on public networks following regulations have to be maintained.

1. All publicly available systems shall be tested against for vulnerabilities, and it shall be ensured that the identified vulnerabilities are fixed prior to publishing any information in such systems.
2. The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification
3. Authorization process according to the cryptographic controls shall be applied at critical end points.

Protecting application services transactions

Information involved in application services transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

1. A secure communication channel shall be set up between all involved parties for application services transactions to ensure that the transactions and parties remains confidential.
2. User's secret authentication information shall be used for verification, authentication and for gaining access to applications.
3. Protocols used to communicate between all involved parties shall be secured.

Correct processing in applications

Input data validation

1. The system acquisition/development methodology of the organization will ensure that appropriate input data validation controls are existing/built-in the systems, prior to their deployment in the production environment.

Control of internal processing

1. **[Entity Name]** production systems shall be built so that all the critical transactions processed shall have a maker who processes the transactions and a checker who validates the transactions before executing it. Clear segregation of duties to be built in the login of application.
2. Privileges shall be established such that only authorized users able to modify production data with necessary approvals.

Message integrity

1. Controls shall be built in the application so that message integrity is maintained.

Output data validation

2. Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstance.

Security of system files

Control of operational software

1. Users shall not write computer programs into production environment unless specifically authorized by the **[Information Security Section/Department or the function assigned with information security responsibilities]**

2. All security fixes provided by software vendors and identified for implementation shall go through a change management procedure.
3. Users shall not install new or upgraded operating systems or application software on personal computers or other machines used to process **[Entity Name]** information.

Access control to program source code

1. Entity shall implement the necessary security controls are implemented to protect the source code including code check-in and code check-out.
2. **[Entity Name]** operations staff will not be given any access to production data, production programs, or the operating system beyond that which they need to perform their jobs.

Security in development and support processes

Secure development policy

1. Security of the development environment
2. Identification of security requirements in early phases of software development
3. Security checkpoints within the project milestones (as applicable)
4. Secure repositories and security in the version control
5. Secure coding standards shall be considered where relevant and mandated for use
6. **[Entity Name]** shall obtain assurance that the external party involved in development will comply with the above rules for secure development (wherever applicable).

Technical review of applications after operating system changes

1. **[Information Technology Section/Department or the function assigned with information technology responsibilities]** shall configure production servers with only authorized operating systems and approved configurations.
2. All production systems shall be regularly reviewed for installing all newly released systems software patches, bug fixes, and upgrades in line with the host hardening checklist.
3. Integrity and application control procedures will be reviewed to ensure that they are not compromised by operation platform changes.

4. **[Information Technology Section/Department or the function assigned with responsibilities of information technology management]** will ensure that appropriate changes are made to the business continuity plans.

Restrictions on changes to software packages

1. Prior to being installed, new or different versions of the operating system and related systems software for multi-user production computers will go through the established release and change management procedure.

Secure system engineering principles

1. Security shall be designed into all architectural layers i.e., business, data, application and technology to balance the need for information security and with the need for accessibility.
2. New technology will be analyzed for security risks and the design will be reviewed against known attack patterns.
3. Secure SDLC procedures will be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security.
4. Security engineering procedures will be applied to outsourced information systems through contracts and bidding agreements between the organization and the supplier to whom the organization outsources.
5. Ensure test data and accounts are removed completely before the application is moved into production state.

Outsourced Software Development

1. Third parties who develop software for **[Entity Name]** will be bound by a contract/agreement ensuring that **[Entity Name]** confidentiality and intellectual rights are protected. Source code escrow may be assessed if required.
2. Third party shall adhere to **[Entity Name]** secure engineering principles
3. **[Entity Name]** shall hold sole custody of the source code and source code backups.

Supply Chain Management

1. **[Entity Name]** shall perform evaluation of suppliers of information systems, system components, medical devices and services and agree with suppliers on control measures and include them in the supplier contract
2. **[Entity Name]** shall check for product compliance with applicable laws, regulations, circulars and standards
3. **[Entity Name]** shall have contracts/agreements in place with all suppliers including but not limited to:
    - Right-to-Audit clause
    - Non-disclosure requirements
    - Terms to comply with entity information security policy and requirements
    - Terms to comply with relevant federal and local government requirements
    - Change of scope in the contractual requirements.

System Acceptance testing

1. Acceptance testing criteria should be established for new information systems, upgrades and new versions
2. Before being applied, patches for production information systems will be examined and tested to make sure they are efficient and have no side effects that might compromise their intended operation.

Encryption Requirements

1. The need for encryption shall be identified by information owners based on the evaluation of information assets in terms of confidentiality, Integrity and availability, as per the information assets classification policy of the Entity.
2. Key strength used should be sufficient to prevent attacks targeted to breaking the cryptographic key (e.g., brute force attack on the cryptographic key)

Key Management

1. Key management that involves the generation, creation, protection, storage, exchange, replacement, and use of Cryptographic Keys
2. In order to mitigate such scenarios, the following standards need to be kept in mind when working with keys (wherever applicable):
    a) The secret key will be secured by logically and physically securing the device on which the key is stored.
    b) The shared secret key will be accessible only by authorized personnel on a need-to-know basis.
    c) Keys will be revoked and generated afresh in case of suspected compromise.
    d) Audit trails of key management activities will be stored and protected.
    e) Internal Certification Authority systems will be managed securely with appropriate physical and logical controls.
    f) Secure backup of private keys will be maintained on an independent secure media which provides a source for key recovery.
    g) Cryptographic keys will be destroyed in a secure manner when they are no longer required.
    h) No copy of user's private key will be retained by the internal Certification Authority to avoid risk of repudiation.
    i) Users shall keep their private keys strictly confidential and shall be responsible for the safety of their private keys.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees, and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**

3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with information security responsibilities]** on a case-to-case basis.

11. Information Security Incidents Management Policy

Objectives

To ensure that entities define and utilize suitable processes and resources to identify and respond to information security and cyber security incidents, that they are not severely impacted by incident outcomes and that they are able to restore affected operations within an acceptable timeframe.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.

Policy Statement

Incident Reporting and Recording

1. All information security incidents shall be reported to the [Information Security Section/Department or the function assigned with information security responsibilities] as per the Entity information

security incidents management procedure (to be developed by the Entity based on the business needs).

2. All information security incidents reported shall be recorded by the [Information Security Section/Department or the function assigned with information security responsibilities] with the relevant details such as:
    a) Detailed description of the information security incident including time of incident.
    b) Details of the user(s) who reported the information security incident including contact details.
    c) Asset/service affected by the information security incident (or thought to have been affected).
    d) Damages observed including any other security events/violations occurred.
    e) Information security Incident status – occurred/ongoing/may occur.
    f) Details on how the information security incident was discovered/detected.
    g) Reference of any similar occurrences in the past.
    h) Supporting evidence.
    i) Remedial steps taken, if any.
    j) Information security Incident classification.

Incident Response

1. After recording the incident details, the **[Information Security Section/Department or the function assigned with information security responsibilities]** shall do preliminary analysis to determine the validity of reported incident.
2. All valid security incidents shall be classified based on the severity by the **[Information Security Section/Department or the function assigned with information security responsibilities]** in consultation with the [Information Security Manager or the job title assigned with responsibilities of managing information security] as Very High, High, Medium, and Low. Refer to information security incidents classification table in policy appendix.
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** shall take corrective actions to contain the incident. If deemed necessary, the

[Information Security Manager or the job title assigned with responsibilities of managing information security] shall inform affected business owners about the incident.

4. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** shall constitute a Computer Security Incident Response Team (CSIRT) for carrying out incident response activities.
5. The CSIRT shall include permanent members, and members designated from other affected business units, based on the asset/service affected by the information security incident and its criticality. Permanent members shall include the **[Information Security Manager or the job title assigned with responsibilities of managing information security],** and other members from the **[Information Security Section/Department or the function assigned with information security responsibilities].**
6. The **[Entity Name]** shall notify Abu Dhabi Health Security Operation Center (SoC) of information security and privacy incidents within predetermined timeframes
7. The CSIRT shall carry out root cause analysis and take corrective actions to contain and eradicate the incident.
8. The outcome of the root cause analysis and all actions taken shall be recorded and a separate database shall be maintained as Security Incident Management Database (SIMDB)
9. Incident shall be monitored from its identification till closure. Based upon the progress, the incident records shall be updated on a continuous basis.
10. Users, customers, stakeholders, and management shall be kept informed about the progress of incidents, as necessary.

Post Incident Analysis and Actions

1. The **[Information Security Section/Department or the function assigned with information security responsibilities]** shall prepare a detailed incident report. This report shall be submitted to the **[Information Security Manager or the job title assigned with responsibilities of managing information security].**
2. Types, volumes, trends, and costs of information security incidents shall be quantified, analyzed and recorded.

3. The outcome of the incident analysis may lead to revaluation of existing policies, development of additional security controls and/or disseminate user awareness programs.
4. The information security incident report shall by default be classified as confidential irrespective of severity or rating of the incident.
5. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** shall advise on the preventive controls to be implemented to avoid the occurrence of similar incidents.
6. All information gained from post-incident analysis shall be recorded for future references.
7. All evidence collected shall be retained for at least 1 year from the time of incident, wherever required the evidence shall be presented to relevant authorities.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from [Information Security Manager or the job title assigned with responsibilities of managing information security] on a case-to-case basis.
5. All Users shall report any known or suspected information security incidents immediately.
6. Anonymity of User reporting a suspected incident shall be maintained unless the matter is referred to a court of law.

Policy Appendix:

Information Security Incidents Classification

1. The below table provides a suggested approach for classifying information security incidents, which can be modified based on the risk and business needs of the Entity:

Priority	Alert Level	Activity Description	Impact
P1	**Critical/Catastrophic** **(Very High Risk)**	Threat of, or actual, malicious cyber activity (hacking, viruses, or other activity) that will disrupt, destroy, or degrade services and infrastructure. Incident occurred, is imminent, or is ongoing. Zero-day exploit has been released and is expected to target entity's systems. The incident will seriously impact entity's Information and related assets or reputation and will require immediate action.	Potential or observed total or near-total destruction, degradation, or compromise of entity's Infrastructure and services. Potential or observed serious and widespread degradation or destruction, threatening continued operation of entity's critical services Known significant impact of zero-day exploit discovery or release exists Normal business operations and functions may be indefinitely suspended Major harm to the reputation of the government. Profound loss of confidence in the credibility, integrity or competency of government, by the citizenry and international partners.
P2	**Severe** **(High Risk)**	Threat of, or actual, increased malicious cyber activity (hacking, viruses, or other activity) directed at national critical service(s) exists. Known or expected targeted intrusion or exploit of an entity providing a national	Potential for or observed major degradation, disruption and/or destruction of entity's Infrastructure and services Potential for or observed high level of degradation, disruption, or damage

		critical service is present or reported Zero-day exploit has been released, The incident affects entity's Information and related assets and should be dealt with as soon as possible. Any incident involving Law enforcement agencies will have an automatic High Impact level.	Impact of zero-day exploit discovery or release is unknown.
P3	**Elevated** **(Medium Risk)**	Threat of, or actual, increased malicious cyber activity (hacking, viruses, or other activity) exists. Known (suspected exploiting known vulnerabilities and weaknesses) or expected intrusion or focused attack is present or reported. Zero-day exploit discovery or release is expected.	Limited or intermittent loss of confidence by citizens and other stakeholders in the design and execution of government services. Potential for or observed compromise and/or service is diminished in entity's Infrastructure and services Potential for or observed moderate level of degradation, disruption or damage with likelihood for more degradation, disruption, or damage. No significant impact has occurred from zero-day exploit.
P4	**Normal** **(Low Risk)**	Threat of, or actual, malicious cyber activity (known hacking, viruses or other malicious activity) presents only a general concern The Incident that does not affect any elements of the entity's Information and related assets but may initiate certain action and should be monitored in case of any change in the impact levels.	Non-critical systems are affected; critical services are not targeted or affected Potential impact is manageable by the responsible owner/operator

Information Security Incidents Reporting Matrix

		Incident Acknowledgement	Incident Resolution	Incident Notification to AD Health SOC	Incident Updates to AD Health SOC	Incident Resolution Communication to AD Health SOC
P1: Critical/ Catastrophic (Very High Risk)	**SLA**	Within 30 mins of incident communication /observation	Within 2 hours of incident acknowledgement	Near-Real Time	Near-Real Time	Within 30 mins of incident resolution
	Mode of Communication	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone
	Responsible Stakeholder	Help Desk/User	Information Technology/ Information Security	Entity Point of Contact	Entity Point of Contact	Entity Point of Contact
P2: Severe (High Risk)	**SLA**	Within 1 hour of incident communication /observation	Within 4 hours of incident acknowledgement	Within 1 hour of Incident acknowledgement	Every 1 hour	Within 1 hour of incident resolution
	Mode of Communication	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone
	Responsible Stakeholder	Help Desk/User	Information Technology/ Information Security	Entity Point of Contact	Entity Point of Contact	Entity Point of Contact

P3: Elevated (Medium Risk)	**SLA**	Within 1 hour of incident communication /observation	Within 24 hours of incident acknowledgement	Within 1 hours of incident acknowledgement	Every 2 hours	Within 4 hours of incident resolution
	Mode of Communication	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone
	Responsible Stakeholder	Help Desk/User	Information Technology/ Information Security	Entity Point of Contact	Entity Point of Contact	Entity Point of Contact
P4: Normal (Low Risk)	**SLA**	Within 1 hour of incident communication /observation	Within 48 hours of incident acknowledgement	Within 24 hours of incident acknowledgement	Every 24 hours	Within 8 hours of incident resolution
	Mode of Communication	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone
	Responsible Stakeholder	Help Desk/User	Information Technology/ Information Security	Entity Point of Contact	Entity Point of Contact	Entity Point of Contact

Incident Acknowledgement: The average time it takes to acknowledge and prioritize a possible security incident.

Incident Resolution: The average time it takes to fully resolve an incident. It shall be calculated from the time the incident gets acknowledged.

Incident Notification to AD Health SOC: The average time in which the entity shall notify DoH- AD Health SOC about the incident. It shall be calculated from the time the incident gets acknowledged.

Near Real Time (Incident Notification to AD Health SOC): Once the incident is acknowledged, the entity will promptly notify the Department of Health - AD Health SOC, ensuring minimal delay between incident acknowledgement and notification to the aforementioned department.

Incident Updates to AD Health SOC: The average time in which entity shall provide updates to DoH about incident status and measures being taken. It shall be calculated after notifying DoH- AD Health SOC about the incident

Near Real Time (Incident Updates to AD Health SOC): Upon communicating the incident to DoH - AD Health SOC, the entity shall promptly provide continuous updates regarding the resolution of the incident to the DoH - AD Health SOC department without any delay

Incident Resolution Communication to AD Health SOC: The average time in which the entity shall notify DoH- AD Health SOC about the incident resolution. It shall be calculated from the time the incident gets resolved

Incident handling team/members (Sample)*

Name of the employee	Team	Contact number	Contact email
XXXX	IT	XXXX	XXXX
XXXX	EMR	XXXX	XXXX

Incident Escalation Matrix (sample)*

			[Entity Name] Internal Escalation Path			External Escalation Path			
Priority of the Incident (P1, P2,P3,P4)	Incident Description	Expected resolution time	Escalation – Level 1	Escalation – Level 2	Escalation – Level 3	Escalation – Level 1	Escalation – Level 2	Escalation – Level 3	Remarks
			Authorized employee	Authorized employee	Authorized employee	DoH- AD Health SOC	DoH- AD Health SOC	DoH- AD Health SOC	

*To be updated by **[Entity Name]** based on the operating environment

12. Information Systems Continuity Policy

Objectives

To ensure systems, applications and resources are available to support service continuity requirements of identified critical services and processes during abnormal situations or environment.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. Services Owners are responsible for developing Service Continuity (SC) Plans for their respective services in coordination with **[Information Security Section/Department or the function assigned with information security responsibilities].**
7. Service Continuity Team (to be structured by the Entity) is responsible for participating in the recovery drills and verifying the functionality of the applications/processes/tests with respect to the defined and agreed scope.

Policy Statement

Identification of Services Continuity Team Members

1. Service Continuity (SC) Team shall be appointed by the Entity top management to establish, implement and maintain the Service Continuity Management System within **[Entity Name]**.
2. Services Continuity Team members shall be selected from different departments/ sections of **[Entity Name]**, as per the selected scope for implementation.
3. The implementation of the Services Continuity Management System shall be monitored by top management.

Implementing Information Systems Continuity

1. A plan, based on appropriate risk assessment, shall be developed for the overall approach to business continuity. Risk Assessment shall also be carried out for IT and network infrastructure to identify points of failure. Key considerations in such a plan will be:
   a) Identify events that cause interruptions to business processes.
   b) Consider all critical business processes, not just information processing facilities
2. Disruption Impact to **[Entity Name]**, shall be mitigated through identifying information systems and their Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
3. The Disaster Recovery (DR) solution along with processes should be implemented in such a way, so as to provide the infrastructure/service/application to the business within the defined RTO and RPO, which includes the time for invocation of disaster. The DR solution shall ensure the confidentiality, integrity of information remain intact.

Recovery Strategies

1. **[Entity Name]** shall develop recovery strategies for critical information systems to minimize the period of disruption and limit the impacts that such disruptions. Information systems Recovery Strategies should ensure that points of failure within the infrastructure are mitigated, and disruption risks are either eliminated or reduced to the bare minimum.

2. All departments/section will prepare, periodically update and regularly test the Information continuity and recovery plan that specifies how recovery/ alternative strategies will be leveraged so employees can continue operations in the event of a business interruption.

Verify, Review and Evaluate Information Security Continuity

1. The Information systems continuity and recovery plan will be periodically tested following the established procedures to determine the effectiveness of plan
2. **[Entity Name]** will identify the lessons learned and update the Information systems continuity plan accordingly

Redundancies

1. **[Entity Name]** shall identify business requirements for availability of information systems
2. Redundant components or architectures shall be considered wherever availability cannot be guaranteed using the existing systems architecture
3. Redundant information systems shall be tested to ensure the successful failover from one component to another

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

13. Compliance Policy

Objectives

The objectives of this Policy are:

1. To define the process and guidelines to be followed, for the purpose of implementing the statutory and regulatory contractual requirements of **[Entity Name]** related to information security.
2. To comply with the applicable UAE laws, Intellectual Property Rights (IPR), contractual obligations with vendors and contractors.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.

Policy Statement

Identification of Applicable Legislation

1. Based on the risk assessment, **[Information Security Section/Department or the function assigned with information security responsibilities]** shall identify list of legal and regulatory laws pertaining to information security that are applicable to the Entity.
2. List of applicable statutory and regulatory requirements pertaining to information shall be documented and approved by the top management.
3. **[Legal affairs section/department or the function assigned with responsibilities of legal affairs]** shall ensure that adequate clauses in relation to information Security are considered in the standard contract templates used in **[Entity Name]**. The contractual clauses may also include the following minimum controls, based on the criticality of the contract:
    a) Compliance with legal and regulatory requirements.
    b) Compliance with Intellectual property rights requirements.
    c) Compliance with information security policies and procedures.
    d) Clear allocation of responsibilities to all the involved parties.
    e) Statement on Non – Disclosure of information.
    f) **[Entity Name]**'s rights to review and audit the compliance with the contracts.
    g) Adequate Service Level Agreements (SLA), where applicable.
4. **[Entity Name]** contract templates shall be reviewed by **[Information Security Section/Department or the function assigned with information security responsibilities]** to ensure inclusion of information security requirements as mentioned in the above point.
5. **[Information Security Section/Department or the function assigned with information security responsibilities]** shall ensure that proper information security controls are implemented to comply with statutory and regulatory requirements applicable to **[Entity Name]**.

Intellectual Property Rights

1. **[Entity Name]** shall ensures compliance with the Intellectual Property Rights through implementing the following controls:

a) Ensuring that software installed and used in **[Entity Name]** systems is strictly in accordance with the applicable licenses conditions.

b) Conducting periodic information security awareness to **[Entity Name]**'s Users on the importance of protecting **[Entity Name]** IPR as well as any external party IPR, and the risk implication of using pirated or unlicensed software on **[Entity Name]**'s systems.

c) [Information Security Section/Department or the function assigned with information security responsibilities] shall be consulted before acquiring any software vendors/suppliers with whom any IP related data may be shared as part of their services. The [Information Security Section/Department or the function assigned with information security responsibilities] shall ensure inclusion of Intellectual Property Rights related clauses in the contracts/agreements with suppliers.

d) Maintaining records and evidence of procurement and ownership of software licenses.

e) Maintaining an Inventory of all **[Entity Name]**'s assets and identifying the requirements to protect IP rights.

f) Ensuring the usage and inclusion of copyright markings and disclaimer over **[Entity Name]** owned documents or materials, or any other type of written information, in order to present **[Entity Name]** copyright status to the Users or readers of such information.

g) Ensuring that **[Entity Name]** Users are adhering to copyright terms of any external party materials, such as books, articles, documents, movies, etc.

h) Prohibiting **[Entity Name]** Users from installing or using any pirated and unlicensed software on **[Entity Name]** equipment or systems.

i) Ensuring that all contract agreements signed with third parties, contractors and employees are addressing IPR and NDA requirements of **[Entity Name]**.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees and any other applicable UAE Laws in this regard.

2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**

3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.

4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

14. Acceptable Usage Policy

Objectives

The objective of this policy is to outline the controls of acceptable usage of information and information systems of **[Entity Name]**. Adherence to this policy would reduce any potential misuse of information processing facilities of the Entity.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing Entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.

Policy Statement

Acceptable Use of Information

1. Users are permitted to make limited and infrequent use of **[Entity Name]** systems for personal use.

2. Users shall ensure that information regardless of its form (electronic or physical) is classified appropriately to avoid loss of confidentiality & integrity of the information.
3. Users shall not interfere with the functionality and performance of any Information Security policies, technical protocols or rules that compromises **[Entity Name]** information Confidentiality, Integrity, or Availability
4. Users shall ensure that information shall be accessed on a strictly "need to know" basis based upon the classification of information.
5. Users shall refrain from discussing **[The Entity shall specify the classification level of information affected by this control, for example confidential information or restricted information or secret, etc.]** under the following circumstances:
6. In the presence of an outsider or other employees who do not have the 'need to know' that information regardless of the physical location and the medium of communication.
7. While using Internet based communication channels such as public forums, blog sites, social networking sites, public mailing list, etc.
8. Users shall not share or send **[The Entity shall specify the classification level of information affected by this control, for example confidential information or restricted information or secret, etc.]** outside office premises without prior approval from the Entity's respective higher management or the assigned owner of the information.
9. Users shall ensure that proper authorization is obtained from the Business Processes/Information Owner and **[Information Security Section/Department or the function assigned with information security responsibilities]** on the usage of removable media to store and transfer **[The Entity shall specify the classification level of information affected by this control, for example confidential information or restricted information or secret, etc.].**
10. Users shall make use of the Entity's approved file sharing tools/mechanisms for all kinds of electronic information exchange (i.e., sharing documents with a colleague or an external party).
11. Users shall not load, download, print, store, or receive any material of a sexual or lewd nature via electronic means or otherwise will be subject to disciplinary action.

12. Users shall not hack into any systems or accounts that is not permitted (including systems or accounts outside **[Entity Name]**) or attempt to do the same or otherwise breach or attempt to breach any computer or network security measures.
13. Users shall not change the configuration of their hardware or software without the prior approval from **[Entity Name]** Information Technology Department/Section except for cosmetic changes such as color, font, and resolution or display output device.
14. Users shall not use **[Entity Name]** for any personal financial gain or financial gain of the Third Party

Access Control

1. Users shall be aware that all access privileges shall be allocated on a "need to use" basis, only the minimum privileges required for the User's functional role shall be allocated.
2. Users shall refrain from accessing information systems with credentials of other employees or affiliates.
3. Users shall maintain their exclusive access privileges on information systems by not allowing anyone else to operate from their account.

Passwords Usage

1. Users shall not share their passwords with anyone including their colleagues, friends, family members etc.
2. Passwords shall be unique in nature. Users shall avoid using the same password for all systems/applications.
3. Users shall take extreme caution while using passwords in public places or in the presence of other people.
4. Users shall be cautious while entering passwords and ensure that passwords are entered only in the correct password field provided.
5. Users shall ensure that passwords are not stored in clear text in any form.

Electronic Communication Usage

1. Users shall ensure that all electronic communication resources provided by **[Entity Name]** are used for official purpose only.

2. Users shall refrain from using the official electronic communication resources for personal communications/correspondences.
3. Users shall be held responsible for any misuse of electronic communication correspondences from their accounts, arising from non-compliance to the information security policies.
4. Users shall refrain from accessing or using any electronic communication account of other Users, unless it is authorized/delegated by the account owner with proper business justification, and this shall be carried out through the responsible business unit and without sharing the password.

Internet Usage

1. Users should make use of internet primarily for official purposes and to fulfill the obligation towards their day-to-day business operation.
2. Users are not allowed to post statements/information or comments on the internet that could damage the reputation of Abu Dhabi Government and/or their entities.
3. Users shall refrain from using the internet to download, upload or install any software from the internet or any other third parties unlicensed software or program on any hardware/equipment belonging to **[Entity Name]**, unless the User is authorized according to the nature of his/her work.

Desktop & Mobile Devices Usage

1. Users shall ensure using Computer and Mobile Devices officially provided by **[Entity Name]** to fulfill the obligations towards their day-to-day business operations.
2. Users shall refrain from connecting any personal computer devices such as laptops to the official network, while being in the premises of the Entity.
3. Users are not allowed to install any unlicensed or illegal copies of software or applications on the officially provided Computer Devices.

Physical Security

1. Employees shall visibly wear the employee ID card issued by the **[HR section/department or the function assigned with HR responsibilities]** while they are inside the premises of Entity.
2. Visitors shall be escorted at all times by an authorized employee while in **[Entity Name]** premises.

3. Users shall refrain from entering critical areas (such as data center, filing rooms) without having business justification and without authorization from the respective owner.

Information Security Incidents Management

1. Users shall promptly report information security incidents either to **[Information Security Manager or the job title assigned with responsibilities of managing information security]** or any member of **[Information Security Section/Department or the function assigned with information security responsibilities].**
2. Users shall support the information security incident response team, to contain the incident and take necessary corrective & preventive actions.
3. Users shall refrain from tampering any source of evidence or audit logs on information systems that may be required for future audit and prosecution purposes.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

15. Antivirus Policy

Objectives

The objective of this policy is to outline the protection controls from malicious codes (such as Virus, Spyware, malware, Trojans) etc., which may harm Computer Devices and servers of the entity, and to establish the requirements for addressing any problems resulting from such infections.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. **[System Administrators or the job title assigned with responsibilities of systems administration]** who are administering the antivirus system are responsible to implement the policy and centrally monitor and analyze the logs of the system.

Policy Statement

Antivirus Installation

1. The **[Technical support section or the function assigned with technical support]** shall ensure that all Desktops & Laptops are installed & configured with the official antivirus software.
2. The **[System Administrators or the job title assigned with responsibilities of systems administration]** of servers shall ensure that all servers are installed & configured with official antivirus software.
3. The Antivirus software shall operate on a real time basis on all servers, desktops, and laptops.
4. Server machines running exclusively on UNIX-based operating systems where the risk of viruses is minimal, may not have anti-virus software installed.
5. Antivirus software shall be configured to do a full system scan once in a week and a real time scan of all the files from external storage media when they are accessed, copied, or moved.
6. The antivirus software shall be configured to clean the malicious contents automatically.
7. Antivirus software shall be configured to quarantine the infected files if they cannot be cleaned.
8. Antivirus software on the E-mail Servers at the gateway level shall be configured for scanning all internal and external mails.
9. Antivirus scanning shall be enabled automatically as and when the Desktops, Laptops, and Servers are started/restarted.
10. Users shall be trained to use antivirus software. However, Users shall not be allowed to install and un-install or change the configuration settings of the Antivirus Software.

Antivirus software and signature file maintenance

1. New Antivirus signatures shall be applied within 24 hours of release by the vendor.
2. **[System Administrators or the job title assigned with responsibilities of systems administration]** who are administering the antivirus system shall ensure that new signature are updated. Similarly, all relevant network and systems endpoints shall be configured for automatic updates.

3. **[System Administrators or the job title assigned with responsibilities of systems administration]** who are administering the antivirus system shall maintain updated documents required for installation, configuration, and administration of all Antivirus Software components.
4. **[Information Security Section/Department or the function assigned with information security responsibilities]** shall coordinate with external security authorities on latest virus breakouts in the region and shall ensure preventive action is initiated.
5. In case of worm/virus or a malicious content originated from any information system, the respective information system shall be disconnected from **[Entity Name]**'s network as a prevention against spread of virus/worm into the network.

Antivirus Server Security

1. The Antivirus system servers shall be placed in a controlled physical access environment with access to authorized personnel only.
2. Logical (electronic) access to the Antivirus servers shall be restricted to the authorized personnel only.

Third Party Access

1. Third Party personnel shall not be allowed to connect Laptops/Desktops to the **[Entity Name]** network without updated Antivirus signature.
2. The [Technical support section or the function assigned with technical support] shall verify that the third-party user's desktop and laptop do not contain any virus or other vulnerabilities that could affect the **[Entity Name]**'s network before being connected to LAN.

Logging and Monitoring

1. Logging shall be enabled on the Antivirus systems. Antivirus systems parameters and Antivirus log files need to be monitored weekly by the administrators responsible of the antivirus systems.
2. All virus detection incidents shall be logged, along with the action taken:
    - Quarantine
    - Deletion
    - Successful cleaning

3. Antivirus logs shall be stored online for 90 days **or (to be decided by the entity based on the risk, business need and any legal or regulatory requirements applicable to the government entity or the specific information)**, and reviewed by **[System Administrators or the job title assigned with responsibilities of systems administration]** who are administering the antivirus system and verified by the **[Information Security Section/Department or the function assigned with information security responsibilities].**

4. The Antivirus system shall also be configured to do the following:

    a) Send an alert to the **[System Administrators or the job title assigned with responsibilities of systems administration]** responsible of the antivirus systems in case of any malicious content not cleaned and on detecting any new virus breakout.

Incident reporting

1. **[System Administrators or the job title assigned with responsibilities of systems administration]** who are administering the antivirus system shall review and report the identified malicious code/content as per the Information Security Incident Management process, that is to be developed by the entity.

2. Users shall report any malicious content detected, configuration change or any unusual behavior in their systems to the **[Information Security Section/Department or the function assigned with information security responsibilities].**

3. Users shall ensure that if a laptop/ desktop is thought to be infected by a virus, it shall be immediately disconnected from **[Entity Name]**'s network.

Change Management

1. All changes concerning Antivirus server/application and configuration settings shall follow the [Entity Name]'s Change Management Process (to be developed by the entity based on the business needs).

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees and any other applicable UAE Laws in this regard.

2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

16. Clear Desk and Clear Screen Policy

Objectives

The Objective of Clear Desk and Clear Screen Policy is to ensure that information is protected from prying eyes and opportunistic breaches, which may lead to compromise in Confidentiality, Integrity and Availability of the information.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security**] is responsible for development, maintenance, enforcement and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.

Policy Statement

Clear Desk

1. Users shall store paper documents and electronic media that are classified as **[The entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.]** in locked cabinets.
2. Users shall keep their desks clean and clear of **[The entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.]** when leaving the office unattended.
3. User shall ensure that **[The entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.],** when printed or transmitted, shall be removed from printers and fax machines immediately.
4. Users shall ensure to protect the **[The entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.]** incoming and outgoing fax messages, postal mails etc. and do not leave them unattended.
5. Users shall ensure all **[The entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.]** /notices shall not be pinned, on the pin boards in front of the desk and notice boards.
6. Users shall ensure that **[The entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.]** written on the white boards shall be wiped off, once the discussion is complete, and shall ensure that such information is not visible from outside the room during the meeting.
7. Users shall ensure keeping their laptops in locked drawers or cabinets once leaving the office.

Clear Screen

1. Password-protected screen savers shall be activated within 15 minutes **(to be decided by the entity based on the risk, business need)**
2. Application sessions shall be locked automatically after 30 minutes of inactivity until a user's password is re-entered.

3. Users shall ensure that they lock the computer screen when leaving their desks.
4. All workstations shall have password protected screen savers enabled and activated after a defined period of inactivity.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

17. Information/Data Backup Policy

Objectives

The objective of this policy is to define adequate back up requirements for the critical information and data of **[Entity Name]** and ensure their availability in the event of disruption.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. The Business Processes Owners and **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** are responsible for ensuring that the backups are taken as per the operational requirements.
7. The **[Backup team or the function assigned with responsibilities of backup management]** is responsible for scheduling the backups as per the operational requirements defined with business owners.

8. The **[Backup team or the function assigned with responsibilities of backup management]** is responsible for handling backup media.
9. The [Backup team or the function assigned with responsibilities of backup management] is responsible for the implementation of this policy on the day-to-day operations.

Policy Statement

Backup Requirements

1. Information/data Backup requirements of all information systems within **[Entity Name]** shall be identified and documented.
2. Information/data stored locally on Users' computers will not be included in scheduled backup. Thus, Users shall transfer their data onto their network drive folders so that it will be included in the scheduled backup.
3. The Business Processes Owners or **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** shall decide on the minimum back up requirements for their respective information/data and information processing systems.
4. The Business Processes Owners or **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** shall decide on the frequency and type of back up for their respective application, database and operating systems and network devices.
5. The **[Backup team or the function assigned with responsibilities of backup management]** shall record and maintain the backup requirements for all information systems. The details shall include information/data to be backed up, backup frequency, storage media, retention and disposal.

Backup Schedule

1. Backup of information/data shall be taken regularly as defined by Business Processes Owners or **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** to ensure information/data is available in the event of failure of information processing systems.
2. The **[Backup team or the function assigned with responsibilities of backup management]** shall perform a minimum level of backup for each server hosting actual production data as agreed with business owners.

3. The **[Backup team or the function assigned with responsibilities of backup management]** shall ensure that any newly commissioned server into production is included for the minimum level of data backup.
4. In the event of schedule backup failure, the **[Backup team or the function assigned with responsibilities of backup management]** shall ensure rescheduling of backup and shall keep the business owners informed on the same.
5. The **[Backup team or the function assigned with responsibilities of backup management]** shall identify the root cause for the failure of backup and the same shall be documented and shared with Business owner.
6. Backup of systems, applications, devices, etc. shall be taken before and after applying any changes, such as upgrades, patching, etc.

Backup Media handling and storage

1. The **[Backup team or the function assigned with responsibilities of backup management]** shall ensure that separate backup tapes are used for daily, weekly, monthly & yearly backup.
2. All backup media must be clearly identified in a consistent manner.
3. Backup copies of critical data must be maintained at an identified offsite location.
4. The offsite location for storage of backup tapes must be in a separate geographic region Offsite backup must be maintained in a fire-resistant enclosure and must be covered with appropriate physical security.
5. Access to backup media while onsite, in-transit, or offsite must be restricted.
6. If backup tapes are discovered to be damaged or corrupted, then these tapes must be destroyed.
7. All backup media shall be disposed-off in a secure manner at the end of their life, according to their retention period, or if found to be corrupted or damaged, and the disposal procedure must ensure the following:
    - The media is properly degaussed.
    - Labels/tags containing reference to **[Entity Name]** internal information is removed.
    - Tapes and others non-reusable data storage media are physically destroyed.

8. A detailed schedule for the movement of back tapes to offsite location shall be documented and a record for the movement of tapes to & from offsite location shall be maintained.
9. All backup tapes must be regularly transported to the offsite storage location as defined by Business Processes Owners or **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** in coordination with the [Backup team or the function assigned with responsibilities of backup management].
10. Handling backup media must be done according to the manufacturer's recommendations and guidelines to prevent damage.

Backups restore and testing

1. Backup tapes shall be randomly tested for data recovery by the [Backup team or the function assigned with responsibilities of backup management]. Recovery testing shall be done at least once in a year.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.

18. Internet Usage Policy

Objectives

The objectives of this policy are to:

a) Ensure efficient and reliable internet usage for all Users in **[Entity Name]**.

b) Protect confidential information and intellectual properties belonging to **[Entity Name]** and ensure that any risk of exposure is minimized.

c) Manage and improve Users' productivity and optimize the use of information technology infrastructure by controlling and monitoring the use of internet service.

Scope

This policy applies to all Users of **[Entity Name]**.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.

Policy Statement

Internet Service Access Provisioning & De-Provisioning

1. Access to internet service shall be granted as per the **[Entity Name]** Access Control Procedures (to be developed by the entity based on the business needs).
2. De-Provisioning of access to internet service shall be raised as per the **[Entity Name]** Access control Procedures (to be developed by the entity based on the business needs).
3. Internet service access de-provisioning is valid under the following circumstances:
    a) End of employee's service
    b) Contractors completing their engagement.
    c) If requested by the Director of the department which the user belongs to.
    d) If user found to have violated the policy or misused the provided service in any mean.

General Usage

1. Users shall make use of internet primarily for official purpose and to fulfill the obligation towards their day-to-day business operation.
2. Users may use the internet for limited personal use as long that it doesn't violate the entity policy or affect the entity business.
3. Users shall refrain from misusing the internet access through using any automated tools to gain or attempted to gain unauthorized access or entry into any third party's systems or devices.
4. Users shall not use unauthorized means of accessing internet such as personal broad band modems, unauthorized wireless access points etc.,
5. Users shall refrain from engaging in any activity that may result in the disruption of operations of the internet service or information systems of **[Entity Name]**.
6. Users shall refrain from posting, disclosing, or sharing information pertaining to **[Entity Name]** that is specific, proprietary or **[The entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.]** in nature on the internet including online forums, groups, anonymous File Transfer Protocol (FTP) servers or any other open online platform.

7. Users are not allowed to post statements on the internet that could misconstrue the reputation of **[Entity Name]**.
8. Users are prohibited from accessing legally or morally offensive websites that contain or support violence, criminal or illegal behavior, extreme religious or political sentiments or opinions or abusive statements related to social aspects, age, race, gender, rituals, or religious beliefs.
9. Users shall refrain from using nonofficial messaging or chatting channels such as online messenger applications or internet chatting channels while connected to the entity's network.
10. Users shall refrain from using the internet to download, upload or install any software from the internet or any other third party's unlicensed software or program on any hardware/equipment belonging to **[Entity Name]**.
11. Users shall refrain from downloading audio and video files or any non-business-related files.
12. Users shall refrain from attempting to change and/or remove the browser settings configured to use the proxy and any direct dial up connection from a system connected to the network.
13. Users are prohibited from using the internet for their own commercial-related gain(s) that falls outside the scope of their employment or business engagement.
14. Users are not allowed to download, copy, or transmit to/from the internet, any other person's works, documents or any other forms of intellectual property belonging to a third party without the third party' express permission nor shall the Users do any act which may expose the Users or **[Entity Name]** to claims of intellectual property rights infringements.
15. Users shall report any internet usage violations or suspicious activities as per the entity Information Security Incident Management process **(to be developed by the entity based on the business needs).**
16. **[Entity Name]** reserves the right to block any websites considered to be non-secure, non-business related or that may affect the performance of the internet services.

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees and any other applicable UAE Laws in this regard.

2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from [Information Security Manager or the job title assigned with responsibilities of managing information security] on a case-to-case basis.
5. Users shall be aware that the **[Information Security Section/Department or the function assigned with information security responsibilities]** in coordination with the [Networking section or the function assigned with responsibilities of network management] reserve the right to monitor the internet usage to verify compliance to this policy.

19. Password Security Policy

Objectives

The objective of this policy is to define and provide guidelines for Users in choosing secure passwords and identify protection controls of those passwords.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. All **[System Administrators or the job title assigned with responsibilities of systems administration]** are responsible to implement the policy on all Users accounts.

Policy Statement

Users Passwords Security Controls

1. All passwords are categorized **as [The entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.].** Users shall not share or disclose passwords to any user (including Managers, IT administrators, etc.)
2. Passwords shall be unique in nature. Users shall avoid using same passwords for all systems/applications.
3. Users shall set strong passwords matching the following criteria:
   a) Minimum length of password should be eight characters or **[to be decided by the entity based on the risk and business needs].**
   b) Should contain a combination of alpha numeric characters and at least one special character.
   c) Should contain both upper and lower-case characters.
   d) Not to be repeated within a cycle of 3 passwords changes **[to be decided by the entity based on the risk and business needs].**
   e) Not to be easily guessable and must not contain:
      - Names of family members, pets, friends etc.,
      - The name of popular places, (i.e., "Abu Dhabi", "Singapore" or any derivation.).
      - Birthdays and other personal information such as address and phone numbers.
      - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.,
4. Passwords should not be blank or similar to the username.
5. Use of generic ids or group accounts is prohibited to ensure accountability. In case where the business need arises for such usage, one user from the group shall be identified to be responsible for all activities carried out of such accounts.
6. List of generic IDs with owners and Users shall be documented and reviewed by the **[Information Security Section/Department or the function assigned with information security responsibilities].**

7. Users shall take extreme care and diligence while using passwords in public places or in the presence of other people.
8. Users shall be very cautious while entering passwords and ensure that passwords are entered only in the correct password field provided.
9. Users shall refrain from using the "Remember Password" feature of any Information systems/application.
10. Passwords shall not be stored in a form that can be subjected to unauthorized views e.g., written and openly kept on desks, pasted on computer screens with the help of post-aids, etc.
11. Passwords shall not be stored in clear text in the form of scripts, source codes, etc.
12. Users shall report any compromise or suspected changes in their accounts as per the information security incidents management procedures of the entity.

Information Systems/Applications Passwords Configuration

1. All information systems/applications shall be configured to enforce passwords change periodically after minimum of 90 days or **[to be decided by the entity based on the risk and business needs].**
2. Users accounts shall be locked temporarily after consecutive **[Number of attempts to be decided by the entity based on the risk and business needs]** failed login attempts.
3. All information systems/applications shall be configured to not allow the reuse of a given password within a cycle of 3 password changes or **[to be decided by the entity based on the risk and business needs].**
4. All information systems/applications shall be configured to enforce Users to change the temporary/initial password immediately after first logon.
5. All information systems/applications shall be configured to store the passwords in encrypted form.
6. All information systems/applications shall be configured to enforce Users to change their passwords after a password is reset.

Systems Administration Passwords Controls

1. All temporary/initial passwords that are provided by the systems administrators shall be complex and unique.

2. All high privilege and administrator accounts shall not be used for carrying out day to day business operations or activities.
3. Password protected screen saver shall be activated for all Users within 10 minutes of inactivity or **[to be decided by the entity based on the risk and business needs**].
4. Password shall be reset when requested by the authorized user after verification of user identity.
5. **[Information Security Section/Department or the function assigned with information security responsibilities]** shall be kept informed of any request raised for password reset of high privilege accounts.
6. Passwords of all high privilege accounts shall follow the entity defined passwords management procedures **(to be developed by the entity based on the business needs).**

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees, and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.
5. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to perform random checking of passwords to ensure its complexity as defined in the policy.

20. Remote Access Security Policy

Objectives

The objective of this policy is to mitigate the risk of potential exposure of information and information processing facilities of **[Entity Name]** while accessing it remotely through the approved virtual private network or other encrypted channels.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. [Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections] and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.
6. The **[Network section or the function assigned with responsibilities of network management]** is responsible to implement the defined security controls on the Remote Access technology being used by **[Entity Name]**.

Policy Statement

Remote Access Provisioning & De-Provisioning

1. Remote Access to **[Entity Name]**'s infrastructure shall be provided strictly on approval from the [Information Security Manager or the job title assigned with responsibilities of managing information security] and the director/manager of the User.
2. Users shall be granted Remote Access with proper business justification falling under any criteria as mentioned below:
    a) Users who have compelling date to complete tasks/projects.
    b) Users working on tasks/projects which requires remote connection after working hours.
    c) Users of Remote Access shall be provided with an end date to the access. Users requiring access beyond the specified end date shall renew their access.
3. Remote Access de-provisioning is valid under the following circumstances:
    a) Users no longer require access to the relevant network or when the temporary access permission granted to the User expires and no renewal have been requested.
    b) End of employee's service.
    c) If requested by the Director of the concerned department to which the user belongs.
    d) If user found to have violated the policy or misused the provided service in any mean.
    e) If Users have not used the Remote Access for 30 days from the time it has been granted.

Usage Controls

1. Users shall be aware that the remote access is considered as privilege access and all Users provided with remote access shall be governed by this policy.
2. Users shall refrain from sharing or disclosing remote access credentials with any individuals.
3. Users shall be held responsible for any misuse of his/her login credentials.
4. Users shall ensure that devices used to connect to **[Entity Name]** network remotely shall have the anti-virus software enabled.

5. Users shall report any violations or suspicious activities found in the remote access, as per the Information Security Incident Management Procedures of the entity **(that is to be developed by the entity based on the need).**
6. Users shall be aware that all activities carried out using remote access is being logged and monitored.

General Controls

1. Remote Access shall be strictly controlled and monitored by the **[Network section or the function assigned with responsibilities of network management]**
2. Strong authentication mechanism with two factor authentication shall be configured for all Remote Access while accessing information or information system through VPN.
3. The installation and configuration of all software and hardware functionalities related to remote access shall be undertaken by the authorized **[Technical support administrators or the job title assigned responsibilities of technical support].**
4. All Users shall have Remote Access with minimum necessary access rights required.
5. All remote connections made to **[Entity Name]** network shall be done through the approved Virtual Private Network.
6. Users shall refrain from using freeware or shareware applications for remote access or connect remotely to **[Entity Name]**'s network for vendor technical support. Usage of such applications requires approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.
7. Users shall use only the approved web conferencing and desktop sharing applications for the purpose of products demo, POC, etc. **[list of approved applications can be provided].**

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees, and any other applicable UAE Laws in this regard.

2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.
5. Users shall be aware that the **[Information Security Section/Department or the function assigned with information security responsibilities]** in coordination with the [Network section or the function assigned with responsibilities of network management] reserve the right to monitor the usage of all activities carried through Remote Access.

21. Mobile and Portable Device Security Policy

Objectives

The Mobile Device and Portable Device Policy is drafted to govern the use of all mobile computing devices including but not limited to enterprise laptops, tablets, mobile/smart phones, and other Personal Electronic Devices (PEDs) by employees in **[Entity Name]** business environment. The policy establishes the controls that need to be implemented for such devices, from the perspective of employee usage and information security.

Scope

This policy is applicable to all **[Entity Name]** Users, Operating facilities, Information Technology (IT) resources including IT teams, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

Responsibilities

1. The **[Information Security Manager or the job title assigned with responsibilities of managing information security]** is responsible for development, maintenance, enforcement, and endorsement of the policy.
2. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to support the relevant business unit/section in implementation of the defined controls and ensuring compliance with this policy.
3. All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
4. The **[Information Security Section/Department or the function assigned with information security responsibilities]** is responsible to conduct awareness about the policy to Users.
5. **[Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections]** and Business Processes Owners are responsible for ensuring compliance to this policy within their area(s) of concern.

Policy Statement

Use of personally owned mobile devices in [Entity Name] environment.

1. All new devices brought in **[Entity Name]** environment accessing **[Entity Name]**'s information network shall be submitted to the **[Entity Name]** IT function for configuration and vulnerability assessment. **[Entity Name]** IT will decide to configure access to **[Entity Name]** internet on the devices, post verification.
2. For email to be configured on the mobile device or to connect to or access **[Entity Name]** network/ systems through iPad, the user would need to accept the company's acceptable usage policy and e-mail usage policies.

Security Controls

1. **[Entity Name]** shall allow access to company's internet connection only on approved personal devices
2. Users shall not be allowed to download any data on the devices. E-mail attachment shall be configured for read only access.
3. On-screen passwords shall be mandatory on the devices. Passwords shall be configured as per **[Entity Name]** password policy.
4. **[Entity Name]** IT shall implement a technology to logically create a partition in the device. This partition shall segregate user's personal information and applications from official information.
5. Remote data wipe agents will also be installed on the mobile devices by **[Entity Name]** IT to protect corporate data theft in events of device being lost or stolen. The scope of data for remote deletion shall be limited to the official partition only.
6. The usage of official mails would be restricted to the devices which are compatible with the mobile device security policy

Personal Device Management

1. **[Entity Name]** is responsible for protecting data on personal devices is limited to protecting corporate data. In events of device being lost, stolen or being rendered useless otherwise, **[Entity Name]** will not be responsible for the replacement of the device or purchase of a new device.

Use of [Entity Name] Provided Mobile Devices

Prior to use or display of confidential data via **[Entity Name]** provided mobile and portable devices such as laptops, tablets, the following security measures must be in place:

Securing the network

1. All devices be part of the **[Entity Name]** domain.
2. **[Entity Name]** network shall be protected using Network Access Control mechanism to prevent access to any entity information to unregistered devices
3. Devices shall be protected with antivirus software and updated regularly for latest security patches. Centralized client policies (virus scan settings) shall be configured to prevent users from altering the level of protection provided.
4. Users shall be permitted to use only pre-approved software. Any other software installation shall require a business justification, approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]**

Protecting Data in Devices

1. Device must authenticate the user before access is granted to services. Strong password controls shall be implemented
2. Devices must be configured to session timeout after defined minutes of inactivity and must require re-authentication before access to services.
3. Devices shall not be connected to unsecured public wi-fi networks
4. Devices must be configured to lock-out after defined number of incorrect password attempts

Secure Disposal and reuse

1. If the device is no longer required, IT team shall ensure that it is sanitized (securely erased or destroyed). No other method of disposal is acceptable.

User Responsibilities

1. User of personal devices shall not try to gain unauthorized access to **[Entity Name]** services, run port scans, use penetrating testing tools, use any hacking tools in **[Entity Name]** network

2. Users of personal devices shall not allow a third party to intentionally or unintentionally gain access to **[Entity Name]** services
3. Users of personal devices need to ensure devices are patched to the latest version and have appropriate anti-virus product installed
4. Personal handheld devices must be secured against unauthorized usage by using a password. Such a password is not to be shared within or outside **[Entity Name]** premises
5. Users are accountable for their personally owned handheld devices and must protect them to minimize the possibility of loss or theft, unauthorized use, or tampering
6. Employees using smartphone devices/ tablets should not try rooting or jailbreaking the operating systems on these devices for privilege escalation
7. Mobile devices must not be left unattended in an unsecure area

Policy Compliance

1. Any violation or breach to the policy may be subject to Information Security Violation Management Process and/or HR disciplinary procedure, the Code of Conduct for Employees and any other applicable UAE Laws in this regard.
2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from **[Information Security Section/Department or the function assigned with information security responsibilities].**
3. The **[Information Security Section/Department or the function assigned with information security responsibilities]** reserves the right to check the compliance of this policy on a periodic basis.
4. Any exceptions to this policy with valid business justification require approval from **[Information Security Manager or the job title assigned with responsibilities of managing information security]** on a case-to-case basis.
5. Users shall be aware that the **[Information Security Section/Department or the function assigned with information security responsibilities]** in coordination with the [Network section or the function assigned with responsibilities of network management] reserve the right to monitor the usage of all activities carried through Remote Access.

Section 4

Controls Implementation

This section contains detailed information for the implementation of each control. These guidelines assist in the correct implementation of the selected control.

Domain 1 - Human Resource Security

Human resources are critical and valuable assets essential for healthcare delivery, but they are also the weakest link within the entity's security framework. The controls of this domain require entities to take adequate measures to ensure that the right resources are hired, are suitably trained to safeguard patient and organizational interest, and are also relieved of their responsibilities in a manner that shall not impact patients, organizational assets, values, reputation and financial conditions at any time, current or future.

The Human Resource Security domain requires the entity's awareness of the risks related to human resources and provides guidance to the entity to establish adequate contractual, administrative, technical and process-oriented controls to minimize probabilities of:

a) Information leakage

b) Unauthorized access

c) System compromise

d) Misuse of privilege, facilities and information

e) Loss of information

f) Credential sharing and misuse

The entity's management should be aware that human resources are easy targets for social engineering and phishing attacks and can be involved in accidental or deliberate attempts to cause disruptions to the entity's services. The entity management should also specifically evaluate the risk environment created by the use of third party and contract resources.

Risks from administrative and cleaning staff are often ignored but they pose new challenges and threats to entities. The entity's management should apply adequate control measures to address those risks.

The objective of this domain's controls are:

To ensure qualified and competent resources are hired and trained to support secure delivery of healthcare services, and that they are relieved in a manner that does not impact patients, organizational assets, value, reputation and financial conditions at any time, current or in the future.

HR 1 Human Resources Security Policy

HR 1.1 Human Resources Security Policy [B]

The Human Resources Security Policy should support the implementation of the Human Resources Domain controls along the entire employment life cycle: prior to employment, during employment, and at termination or change of employment. The policy can, for example, contain:

a) Specification of the groups to be covered by the scope of the policy all users with access to information assets.

b) Management roles and responsibilities during each phase of the employment life cycle including background verification and enforcing awareness training.

c) Employment terms and conditions including code of conduct / non-disclosure agreements / confidentiality agreements.

d) Mandatory information security awareness and training during employment in line with controls HR 3.2 to HR 3.3

e) Disciplinary process for security breaches.

f) Employment termination procedures and checks including return of assets, access revocation and notification.

Depending on the size and structure of the entity, the Human Resources Security Policy can be included as part of a single general information security policy document or can be split up into multiple policies that reflect the complex nature of the entity.

To facilitate entity policy development process, the DoH has provided sample Baseline Policies in Section 3 of this document. Entities are free to customize the provided baseline policies as per their environment

as long as they remain compliant with the requirements of the ADHICS Standard and any other DoH or legal requirements.

Note that, besides the Human Resources Security Policy, this domain has the following supporting or dependent entity policy references:

1. Information Security Policy
2. Acceptable Usage Policy
3. Compliance Policy

HR 2 Prior to Employment

HR 2.1 Background Verification [B]

Subject to restrictions from privacy and employment legislation, background verification checks should be conducted on all candidates for employment as well as for contractors and third-party staff.

This verification is to be conducted by the entity independent of the checks done by the DoH for health professional licensing as well as the checks done by the Labor and/or Immigration Departments during the visa approval process.

The background verification should result in an accurate capture of an employee's identity, professional credentials and work history. Employee details should be periodically reviewed **[Entity shall decide the review Frequency]** to ensure that they are current and accurate, particularly frequently changing fields like contact information and addresses.

Background verification could include a check on the accuracy of the applicant's CV, check on the Primary Source Verfication report, check on academic qualifications and professional memberships, verification of previous employment data and personal references, identity verification as well as police and credit checks. The details to be verified should be defined based on the role of the employee. Where the job entails access to information systems handling healthcare information, financial information or any other highly confidential information, more detailed checks should be done, as required. These requirements should be re-evaluated on change of role or promotion of the candidate. A record of the background verification should be retained for audit purposes.

Privacy of candidates should be respected at all times and only authorized staff should have access to verification data. A procedure should define background verification criteria and process. Candidates should be made aware of this verification requirement.

Where staff are provided by a third party on a contractual basis, the contract with the agency should clearly specify the agency's responsibilities for screening and the notification protocols if background verification is incomplete or fails. The entity's Procurement and Legal Departments may be involved in this.

Throughout the pre-employment process, security duties and responsibilities shall be specified and clearly communicated to prospective candidates

The ultimate aim should be to ensure integrity, competence, professionalism and information security awareness across all levels of staff of the organization

HR 2.2 Terms and Conditions of Employment [B]

The Terms and Conditions of employment may contain general information security requirements common to all employees as well as specific terms and conditions concerning information security appropriate to the nature and extent of access, they will have to the entity's information assets.

The entity should ensure that employees, contractors and third-party user's acceptance of terms and conditions concerning information security is signed and available during audit.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

The entity shall:

a) Include control requirement specific to employees, contractors and third parties, relevant to their roles and risk profiles in the contract

b) Include information security responsibilities of the entity and of the employees, contractors and third parties in the contract

c) Ensure employees sign a Non-disclosure Agreement (NDA) with the entity, as required

d) Ensure the contract includes disciplinary action in case of non-compliance with the information security requirements of the entity

e) Ensure the Terms and conditions is read, understood, agreed and signed by employees, contractors and third parties

f) Conduct mandatory briefing sessions to employees, contractors and third parties on standard and specific information security requirements of the terms and condition

g) Maintain adequate records on employee, contractor and third party briefing

h) Maintain Terms and Conditions, Non-disclosure Agreement (NDA) signed by employee, contractor and third-party resources in-line with entity retention requirements

i) Review and update any existing contract with employees, contractors and third-party users, as required

The access to organizational systems and privileges shall not granted until the terms and conditions of employment have been satisfied and agreements have been signed.

HR 3 During Employment

HR 3.1 Establishing Policies and Procedures [B]

It is an entity management responsibility to ensure new staff are properly briefed on their information security roles and responsibilities. The employee should be made to sign the entity's Acceptable Usage Policy prior to being granted access to entity information assets.

When assigning access to information assets, the entity should always consider separation of duties to avoid potential conflict of interest or misuse of position.

HR 3.2 Awareness Program [B]

Cybersecurity has a similarity to healthcare, in that prevention is better than cure. Increasing staff awareness about secure handling of information assets will prevent a majority of information security incidents and change the entity's security posture from reactive to proactive.

Awareness training can take different forms depending on the size and structure of the entity. It is critical that the material used is relevant and up to date. Innovative methods and incentives can help improve staff participation.

The Department of Health will also contribute to the entity's efforts by providing email tips, posters etc. Entity staff subject to Department of Health licensing procedures shall also undergo Cybersecurity e-learning as part of their Continuing Education (CE)/Continuing Professional Development (CPD) process.

Notwithstanding the support from the Department of Health, it is entity management's responsibility to ensure staff achieve a level of awareness on security relevant to their roles and responsibilities within the entity and are also motivated to fulfill the security and data privacy policies of the entity. The training should be to an annual schedule and a record of awareness training provided should be maintained.

The awareness campaign shall:

a) Present current risks around the work and industry, and ways to address.

b) Present learning from incident

c) Demonstrates the need to protect Health Information

d) Include benefit of information security and data privacy compliance

e) Demonstrate stakeholder responsibilities.

f) Highlight entity, government and regulatory demands

HR 3.3 Awareness and Training [T]

Increasing staff awareness about secure handling of information assets will prevent a majority of information security incidents and change the entity's security posture from reactive to proactive.

Awareness training can take different forms depending on the size and structure of the entity. It is critical that the material used is relevant and up to date. Innovative methods and incentives can help improve staff participation.

The DoH will also contribute to the entity's efforts by providing email tips, posters etc. All entity staff subject to DoH licensing procedures will in the future also have to undergo Information Security and Data Privacy e-learning as part of their annual training programme.

Notwithstanding the support from the DoH, it is the entity's management's responsibility to ensure all the licensed healthcare professionals complete the training courses assigned to them by DoH

These skill and competency gaps have to be identified and addressed by providing training and competency development programs. Such gaps can be identified by a risk assessment followed by appropriate remediation.

The training should be to an annual schedule and a record of awareness training provided should be maintained.

HR 3.4 Role Based Training [A]

Users with significant information security roles and responsibilities are required to undergo appropriate role-based information system security training.

The organization shall maintain a documented list of each individual who completes the on-boarding process.

HR 3.5 Disciplinary Procedure [T] [S]

A disciplinary procedure is needed as part of the enforcement of human resources security. After verifying the security incident and identifying the employee responsible, a graduated response based on the risk exposure and employee history is recommended. Breaches can be intentional or accidental and the two should be treated differently.

An incident resulting in loss or leakage of health data should be considered a critical incident and may render the employee liable for instant dismissal. Such incidents may come under the purview of Federal Law No. 2 of 2019 on the use of ICT in healthcare.

A record should be maintained of all security incidents and of actions taken in response by management.

HR 4 - Termination or Change of Employment and Role

HR 4.1 Termination Responsibility [B]

A common security failure during the employee exit process is the failure to inform all stakeholders. This can result in physical or logical access being allowed after the exit date.

An internal and external communication protocol on employment exit is required so that all internal and external stakeholders are informed. Internal stakeholders should be informed about knowledge transfers and responsibility handovers. The employee should ensure employee handover entity data prior to their exit.

External stakeholders like the DoH and the Health Information Exchange, etc. should be informed where applicable.

The organization should get the exit clearance form filled and signed by following section/department SPOCs before employee exit:

a) Human Resource

b) Admin

c) Information Technology

d) Finance

e) Reporting/Line Manager

Change of contract and employee section/department should be managed as the termination of current employment, and the new responsibility should be handled like a new employment.

HR 4.2: Return of Assets [B]

The scope of this control covers physical and information assets. All issued software and hardware should be recovered as part of the employee exit process. This process can be efficiently completed if an asset management system is in place (see AM 2.1).

Possible items include computers, mobile phones, electronic storage media, medical equipment, access cards, licenses, keys etc. All entity information, especially healthcare related information should be recovered. If personal equipment was used to store such information, the data should be transferred to

entity equipment and then securely erased from personal equipment. The handover should also include documentation of operational knowledge including passwords where applicable.

The confirmation of recovery should be signed off by relevant internal stakeholders and the departing employee should also confirm in writing that no entity data is in his direct or indirect control.

HR 4.3 Removal of Access Rights [B] [S]

Due to the sensitive nature of healthcare information, entities should consider immediate termination of access rights following resignation, dismissal, etc., or wherever an increased risk is perceived. In some cases, it may be acceptable to allow restricted access before the final exit. Such a situation should be carefully evaluated considering the reason for the termination, their current access, and responsibilities.

Written instructions from entity management or authorized staff should be followed for access termination in all cases.

As part of the termination process, access that should be removed include physical and logical access. For example, keys, identification cards, information systems, medical equipment, subscriptions, biometric security systems, as well as removal from any documentation that identifies them as a current member of the entity. Any common password shared with the employee should also be changed upon exit, particularly for medical equipment.

Where applicable, the entity should communicate with the DoH, Health Information Exchange (HIE)Abu Dhabi government to revoke any relevant system and application access upon termination.

HR 4.4 Internal Transfers and Change of Role [B]

Upon internal transfer, all access rights of an individual to assets associated with information systems and services should be reconsidered. Change of employment should be reflected in removal of all access rights that are not explicitly approved for the new role.

The access rights that should be removed or adapted include physical and logical access, keys, identification cards, information systems, medical equipment, subscriptions, biometric security systems and removal from any documentation that identifies them as a current holder of the old role. If the employee, contractor, or third-party user has known passwords for common accounts, these should be changed where access is to be removed.

Domain 2 - Asset Management

Asset Management is key to effective Health Information Security management. Entities are witnessing an influx of new asset classes that are very different from the ones they are used to dealing with. Innovative care delivery mandates that entities and professionals deal with a large number of relatively small, mobile and sophisticated pieces of equipment/devices, and to keep them running at all times as they are often critical to the patient's health, safety and wellbeing. In order to be effective and supportive of organizational business and security objectives, entities should maintain an updated version of asset inventory. The current version should be available to relevant management, business, and support stakeholders.

Information assets includes information/data in all its forms, as well as the underlying application, technology, and physical infrastructure to support its processing, storing, communicating, and sharing.

The following are considered information assets:

a) Information (in physical and digital forms)

b) Medical device and equipment used for diagnosis, therapy, monitoring, rehabilitation, and care etc.

c) Applications and System Software

d) Information System

e) Network Infrastructure Devices

f) Services and Processes

g) Virtual Infrastructure

h) Physical Infrastructure (Data center, access barriers, electrical facilities, HVAC systems, etc.)

i) Human resources (in support of services/care delivery)

<u>The objectives of this domain's control are:</u>

The regulatory structure surrounding nearly every facet of the healthcare operations, from protecting patient data and improving health outcomes, to reporting on compliance-related issues, necessitates entities to monitor and record the use of information assets.

AM 1 Asset Management Policy

AM 1.1. Asset Management Policy [B]

The Asset Management Policy provides a structure for the management of IT assets (e.g. people, hardware, software, data, facilities) from procurement to disposal. The policy can, for example, contain:

a) IT assets classification scheme (DoH Standard)

b) Classified assets security requirements

c) Disciplinary procedure

Additional policy controls for medical devices and equipment are covered in AM 1.2.

Depending on the size and structure of the entity, the Asset Management policy can be included as part of a single general information security policy document or can be split up into multiple policies that reflect the complex nature of the entity.

To facilitate entity policy development process, the DoH has provided sample Baseline Policies in Section 3 of this document. Entities are free to customize the provided baseline policies as per their environment as long as they remain compliant with the requirements of the ADHICS Standard and any other DoH or legal requirements.

Note that, besides the Asset Management Policy, this domain has the following supporting or dependent entity policy references:

1. Data Retention and Disposal Policy
2. Physical and Environment Policy
3. Portable Device Security Policy
4. Acceptable Usage Policy

AM 1.2 Allocation of Medical Assets [B] [S]

These additional controls specific to medical devices and equipment are to be taken into account when developing the asset management policy mandated by AM 1.1.

Medical equipment and devices play a crucial role in the treatment and diagnosis of illness and disease. However, as discussed elsewhere in this document, they also introduce new risks. This control is intended to help manage the risk associated with the use of medical equipment and devices. Specific attention to access control, authentication, authorization, handling procedures, risk log and disposal of medical equipment and devices is required as part of this control.

This can be included as part of the asset management policy, in a single policy document, or can be represented by a separate policy reflecting the complex nature of certain entities.

AM 2 Management of Assets

AM 2.1 Asset Inventory [B] [S]

The entity should have all their information assets identified, recorded, and maintained through an information asset inventory.

The inventory should be updated periodically, or during change in the environment, and should be accurate and reliable. The inventory can be centralized or distributed based on the entity's internal structures. To achieve consistency across the entity, current version of each inventory should be available to all stakeholders.

A typical list of inventory assets that might be considered include but is not limited to:

a) IT Assets i.e. Laptops, workstations, storage, servers, security devices (firewall, IDS/IPS, anti-spam, etc.)

b) Network assets i.e. Routers, gateways, switches, wireless access points, printers etc.

c) Staff - Information Technology Director/Manager, Database architect/administrator etc.

d) Internal applications - Electronic medical records (EMR), Financial control, ERP, CRM, email etc.

e) External facing applications - Websites, Mobile Apps, E-commerce, IP addresses, DNS services, etc.

f) Medical devices and equipment

g) Data - Customer personal data, customer health data, entity's employee personal and

h) financial data

i) Physical facilities - Hospitals, medical centers, clinics, pharmacies, data centers, etc.

AM 2.2 Asset Relationship [A]

The inventory should establish the relations between various types of information assets, in support of care delivery.

Sample illustration: Service A => needs B Information => supplied by C Device/Equipment/Process/Dependent-Service => processed using D Application (ERP/EMR/Office Automation Applications/etc.) => running on E Technology (server/systems) => supported/operated/managed by XYZ Roles (human resources involved in care delivery)

AM 2.3 Asset Ownership [B]

Every identified asset should be assigned an 'Owner'. The owner maybe an individual or a designated role. The purpose is to assign responsibility for the security of the asset.

The responsibility of the 'Owner' should be to:

a) Define/identify the control requirements to minimize the impact of risk, due to the compromise of assets under his/her ownership.

b) Review the adequacy of implemented control measures periodically and amend/modify the control environment as necessary.

c) Ensure effectiveness of the implemented controls, in addressing the risk environment.

d) Authorize access and/or use of information assets.

e) Define and periodically review access restrictions and classifications, in line with the access control policy of the entity.

Note that the patient is the final owner of his/her personal healthcare information and 'Owner' designated by the entity acts on behalf him/her.

Ownership of shared IT resources (email system, Active Directory, Common File Server, etc.) should be collectively owned by the entity's Information Technology/System or Information and Communication Technology Function.

AM 2.4 Acceptable Use of Assets [B] [S]

The entity should establish and enforce rules on the acceptable use of information assets.

a) The rules should be communicated to all employees, contractors and third-party users in support of care delivery, and should be read and acknowledged by all.

b) Entities should maintain records of user acceptance on the acceptable use of information assets.

The policy should consider general requirements and industry best practices and should have management requirements to reduce probabilities of information leakage/loss/theft and system compromises.

AM 2.5 Acceptable Bring Your Own Device Arrangements (BYOD) [B] [S]

Entity management should be aware of emerging cyber risks and should address risk due to the exploitation of the concept-in-practice "Bring Your Own Device (BYOD)". While BYOD is considered user friendly and cost effective, use of personal devices introduces a major risk. The range of devices with different operating systems and applications means that entity data is exposed to various vulnerabilities.

The entity shall reduce probabilities of compromise and address BYOD related risks through suitable controls and role-based usage agreements. Authorization to use personal devices to access/view/use/share/process/store PII and PHI is subject to user acknowledgement on the usage agreements.

Control process and technology solution should be implemented to reduce/address/contain factors of risk.

The entity should consider implementing a robust mobile device management (MDM) solution, depending on its operating and risk environment, to securely access PII and PHI

Health Information. MDM should be able to containerize and fully separate entity information from user personal information.

AM 3 Asset Classification & Labelling

AM 3.1 Information Classification [B] [S]

An entity shall classify its information assets based on the below classification scheme or using the predefined entity's classification scheme approved by entity management, provided that it is aligned with the classification factors and criteria as defined below:

a) Red = Secret

b) Orange = Confidential

c) Blue = Restricted

d) Green = Public

The DoH standard colors for classification used for visual representation as given above. See also Section AM 3 of the ADHICS standard as well as the Information Asset Management policy in the Baseline policies in Section 3 of this document.

In addition to the traditional classification of health data based on its sensitivity to disclosure, the criticality of information also needs to be classified, i.e. the extent to which the availability and integrity of the information are essential for the ongoing provision of healthcare. Time factors involved in the treatment processes often play a crucial role in determining the availability requirements for healthcare Information. Classification in respect of confidentiality, availability and integrity should also be applied to IT equipment, software, locations and staff. The requirements of protection for information assets in healthcare is unique and should not be compared with standard government or military data classification systems.

Criticality of information assets should be identified through a risk assessment tool/exercise. **See ADHICS Section A-4, Information Security Risk Management.**

Classification is the responsibility of the designated 'Owners' of information assets. The scheme should be consistent across the whole entity so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection.

The entity should establish process to label its information assets in all its form in a way that is consistent with its classification scheme.

Procedures for information labeling should cover information and its related assets in physical and electronic formats. The labeling should reflect the classification scheme in which it is established. The labels should be easily recognizable. The procedures should give guidance where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media. The procedures can define cases where labeling is omitted, e.g., labeling of non-confidential information to reduce workloads.

Output from systems containing information that is classified as being confidential or secret should carry an appropriate classification label in the output. Since all PII and PHI is classified as confidential, output from medical equipment and devices should be labeled as such at the output.

The entity should establish process to reassess and/or change information classification, based on the following:

a) Change in the value of information.

b) Changes to environment (location, access, storage, processing, usage, etc.)

c) Changes in protection levels

Asset classification should be updated in accordance with changes of their value, sensitivity, and criticality through their life cycle.

AM 3.2 Interpretation of External Entities Classification Scheme [T]

The entity should establish process to interpret classification schemes, while receiving information from other entities/3rd parties and should apply all essential control measures to safeguard/protect against compromise.

The DoH has mandated a common classification scheme for the Abu Dhabi healthcare sector. The ADHICS standard also mandates visible and digital indications of the current classification. This will simplify the sharing of data without risking its security.

AM 3.3 Asset Tagging [T]

The entity should have a process to tag its information assets with unique tags (or a label, barcode etc.) prior to deployment in the entity environment. The asset tags can be used for tracking, inventory, and accountability purposes.

Asset tags go hand in hand with some form of a digital scanning system that transfers information off the label to a digital asset management system and/or end user.

AM 4 Asset Handling

AM 4.1 Handling Procedures [B]

Handling procedures should be defined for information, consistent with their classification. Keep distribution to a minimum as required for entity operations. All media should be clearly marked with the intended recipient. Care should be taken that the classification scheme used within the entity may not be equivalent to the schemes used by other entities, even if the names are similar; in addition, information moving between entities may vary in classification depending on its context in each entity, even if their classification schemes are identical.

a) Handling procedures should detail security requirements during:
    - Access granting and privilege allocation.
    - Processing
    - Storing
    - Communication/sharing

- Printing

b) Security requirements based on asset criticality should be considered in the handling procedures.

AM 4.2 Management of Removable Media [B] [S]

The entity should manage removable media in accordance with the classification scheme, handling procedures and acceptable use of assets.

Removable media can be a source of data leakage and the entity should limit the use of removable media to those with a valid business need upon encryption of data.

The entity should:

a) Establish media management procedures to address lifecycle requirements (setup, distribution, utilization, and disposal)

b) Implement rules and guidelines for protecting assets against unauthorized access, misuse or corruption during movement.

c) Ensure accountability for information system media while it is being transported outside of restricted locations.

d) Accept all involved/inherent risk concerning the use of removable media, and shall bear all responsibilities and is held accountable for the risks inherent in authorizing the use of removable media.

AM 4.3 Access Allocation for Medical Devices [B] [S]

Access and privilege allocation for medical devices should be provided to defined roles, with essential qualification and experience required to operate. Medical equipment and devices should be protected from unauthorized operation. Where available, access should be restricted with passwords following the entity password policy.

The entity should:

a) Secure and safe-guard medical devices and equipment in accordance with its classification scheme and risk factor.

AM 4.4 Security of Information within Medical Devices [T] [S]

The Medical devices and equipment often collect and process sensitive Health Information. The entity should prevent unauthorized disclosure, modification, destruction or loss of patient healthcare information stored on medical devices and equipment. While security measures such as encryption are essential to guard against hackers, entity must also ensure that Health Information is not lost or stolen through employee's neglect or malicious intent.

AM 4.5 Communication Facility for Medical Devices [T]

Healthcare facilities should consider wired communication facility for medical devices and equipment. Usage of wireless communication facility with medical devices and equipment should be avoided to the extent possible.

Use of wireless networking introduces the possibility of Denial of Service (DoS) attacks as well as Man in the Middle (MitM) attacks which can affect the availability and confidentiality of data on the internal network. This is especially critical for medical devices and equipment. See also CM 5.4. If wireless networks are used, then the strongest available authentication and encryption should be used. Connections should be logged, monitored, and restricted to trusted devices.

AM 4.6 Removable Media Security [A]

Entity should deploy technology solution to control and monitor removable media and should be complemented by content encryption and biometric based access provisioning. The entity should always consider the data leakage risks from removable media.

AM 4.7 Removal and Movement of Information Assets [T] [S]

The entity should establish control procedures for the removal, movement, and transfer of information assets (information, equipment, medical devices, and information processing equipment/systems).

The entity should:

a) Authorize removal, movement, and transfer of information assets. Equipment, information, or software should not be taken off-site without prior authorization.

b) Maintain records of removal, movement, and transfer for audit purposes.

AM 5 Asset Disposal

AM 5.1 Information Asset Secure Disposal [B] [S]

The entity should dispose of information assets, when no longer required:

a) by the entity

b) on basis of regulatory demands or

c) for legal proceedings

The retention demands of various healthcare laws and regulations should be followed before physical or digital data is disposed. Data on media marked for disposal should have passed the retention period or should be available on a verified backup or archive. However, disposal should be done on a regular basis as retaining media indefinitely may create a security weakness considering the potential volume of data that will accumulate.

Due to the sensitivity of Health Information PII and PHI, it is recommended that media both digital and physical, containing entity data be physically destroyed. Reuse of digital media for entity internal use maybe acceptable provide military grade wiping tools have been used to wipe the media. The entity shall ensure sensitive data and licensed software has been securely removed beyond recovery, prior to disposal.

All disposal requirements should be authorized by entity management prior to disposal. Formal procedures for the secure disposal of media should be established to minimize the risk of confidential

information leakage to unauthorized persons. In the context of an entity all media for disposal should be treated as confidential. Destruction of media by a third party should be supervised and the third party should issue a certificate of destruction.

AM 5.2 Records on Disposal [T]

The entity should maintain records, on media disposal. The records should be available for audit purposes for a period defined by the retention policy. Appropriate controls should be implemented to protect records and information from loss, destruction, and falsification.

The records should have, but not be limited to, the following fields:

a) Information and/or asset owner

b) Type of media

c) Classification

d) Disposal type

e) Reason for disposal

f) Retention expiry date (if data)

g) Data removal confirmation and evidence

h) Disposal authorized by

Domain 3 - Physical and Environmental Security

Physical and environmental security measures shall be implemented to ensure processing facilities are physically protected from unauthorized access, damage, interference, and equipment are protected from physical and environmental threats.

These security measures and controls shall protect entities from loss of connectivity, availability of information processing facilities, storage (backup and archival) equipment(s)/facilities and medical equipment's/devices caused by theft, fire, flood, intentional destruction, unintentional damage, mechanical failure, power failure, etc. Physical security measures should be adequate to deal with foreseeable threats and should be tested periodically for their effectiveness.

The following aspects of physical and environmental security should be considered.

a) Physical protection of data center and information processing equipment(s)/facilities

b) Physical entry control for secure areas

c) Medical devices/equipment(s) protection

d) Heating, ventilation, and air conditioning of critical areas and workplaces

e) Supporting mechanical and electrical equipment's

f) Surveillance of critical areas and workplaces

g) Security and protection of physical archives

h) Fire and environmental protection

i) Visitor management

The objective of this domain's controls are to:

To ensure that information assets receive adequate physical and environmental protection, and to prevent or reduce probabilities of physical and environmental control/security compromises (loss, damage, theft, interference, etc.)

PE 1 Physical and Environmental Security Policy

PE 1.1 Physical and Environmental Security Policy [B]

The entity should develop, implement, and maintain a physical and environmental security policy, to ensure adequate physical and environmental protection of entities information assets. The policy should:

a) Be relevant and appropriate for entities operational and risk environment, concerning internal and external threats.

b) Address requirements of secure storage of hazardous or combustible materials that ensures avoidance of:

- human injuries or loss of life
- damage to information and information systems

c) Consider classification of information assets and their physical presence

d) Define roles and responsibilities for actions expected out of physical and environmental security policy.

e) Be reviewed, updated and maintained at planned intervals or during significant changes to operating or risk environment, whichever is earlier.

f) Be read and formally acknowledged by all user.

g) Be approved by entity's top management or head of the entity, and should be communicated to all employees and third parties having role in care delivery.

Additionally, the controls specified in PE 1.1 for medical equipment should also be taken into account while defining this policy. Adherence to the recommendations of the manufacturer medical equipment and devices as well as applicable regulatory requirements should be mandatory. Placement and physical access should take into account hazards of certain medical equipment like radiation, strong magnetic fields as well as bio-hazards. Protection of Personal Information during maintenance, decommissioning and/ or authorized off-site activities should be covered as well.

Depending on the size and structure of the entity, the Physical and Environmental Security policy can be included as part of a single general Information Security Policy document or can be split up into multiple policies that reflect the complex nature of the entity.

To facilitate entity policy development process, DoH has provided sample Baseline Policies in Section 3 of this document. Entities are free to customize the provided baseline policies as per their environment as long as they remain compliant with the requirements of the ADHICS Standard and any other DoH or legal requirements.

Note that, besides the Physical and Environmental Security Policy, this domain has the following supporting or dependent entity policy references:

1. Clear Desk and Clear Screen Policy
2. Data Privacy Policy

In addition to the Physical and Environmental Security Policy, entities classified as transitional or advanced should develop, document, and implement matching procedures and guidelines.

The procedures should facilitate the implementation of the physical and environmental security policy and associated physical and environmental protection controls.

The following sample guidelines can be considered to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:

a) Hazardous or combustible materials should be stored at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area.

b) Fallback equipment and backup media should be sited at a safe distance to avoid damage from a disaster affecting the main site.

c) Appropriate permanent and portable firefighting equipment should be provided and suitably placed.

PE 2 Secure Areas

PE 2.1 Physical Security Perimeter [B] [S]

The entity should define and use security perimeters to protect facilities that contain information and information systems. Particular attention should be provided for PII and PHI

The entity should:

a) Identify secure areas (e.g., Data center, ICU, surgery rooms, Drug store, Record rooms, Radiology labs, CCTV rooms, Record rooms etc.) and define security perimeter, based on information assets contained within or information being processed. The design of the perimeter should be based on the size of the facility and the layout.

b) Ensure adequate security counter measures are applied to identified secure areas to protect information and information systems within. Counter measures could include solid doors, bars, alarms, locks etc. Biometric security and CCTV systems can also be used. Manned reception and security desks with staff trained to allow only authorized personnel access.

c) Secure areas where medical equipment and devices are installed or used should be protected to avoid and minimize probabilities of unauthorized access and usage. Physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination. The entity should always ensure that the security measures are selected in a way that ensures security without compromising efficient healthcare delivery.

d) Consider the impact of compromise of confidentiality, integrity and availability of information or information assets while applying security counter measures. The measures undertaken should be proportionate to the risk and impact identified.

e) Ensure USB devices used by third parties for maintenance tasks like firmware updates should be checked prior to being allowed to connect.

f) Implement measures for controlling access of mobile devices, portable devices, and surveillance devices to secure areas pf the entity as:

- Mobile devices, portable devices, and surveillance devices may have access to PII and PHI or be used to capture images or videos that could compromise patient privacy if they are used in restricted areas.
- Mobile or portable devices used in secure areas, may be more vulnerable to hacking or data breaches. Access controls can help prevent unauthorized access to sensitive information.
- Surveillance devices may be used in hospital settings to monitor patients in certain areas. If unauthorized individuals have access to these devices, they may interfere with patient monitoring, which could compromise patient safety.

PE 2.2 Private Areas [A]

Discussion of patient information in public areas like corridors, elevators etc. should be avoided. Secure private areas to discuss personal healthcare information between authorized stakeholders and/or patients can ensure confidentiality and privacy. This requirement is for entities classified as Advanced only.

The areas should be unobtrusive and give minimum indication of their purpose. The rooms should be soundproof. Relevant health and safety regulations and standards are applicable.

PE 2.3 Secure Areas Control Measures [B]

Secure areas involved in information processing and personal healthcare information should be protected by appropriate control measures to ensure only authorized personnel are provided access and authorized activities are being conducted. The recommended controls to achieve this are listed below.

The entity should:

a) Maintain a list of authorized personnel having access to secure areas.

b) Authenticate all persons accessing secure areas.

c) Maintain records for secure area access. This will provide an audit trail to ensure access to these secure areas is controlled.

d) Maintain visitor access logs for visitors to secure areas. At a minimum, visitor access records must include the following information:

- Name and organization of the person visiting.
- Visitor's signature
- Identification proof.
- Date of access.
- Time of entry and leaving.
- Access granted by/accompanied by

e) Ensure that all employees and contractors wear distinguished form of visible identification (Badge/ID cards) within the premises of the entity. This will improve awareness and identification.

f) Ensure the locking mechanisms on all access doors are adequate, and alarms configured to alert prolonged open-state of doors. Monitoring normally closed doors being kept open can identify unauthorized access.

g) Escort contractors or third parties while inside the secure areas. Contractors or third parties should not be allowed to work unsupervised in secure areas.

h) Deploy closed circuit television (CCTV/surveillance camera) in identified vantage points of secure areas as required by Monitoring and Control Centre (MCC) Abu Dhabi.

i) Preserve CCTV footage for a period as required by Monitoring and Control Centre (MCC) Abu Dhabi. The Monitoring and Control Centre (MCC) Abu Dhabi has detailed requirements regarding CCTV coverage of facilities. Compliance to the Monitoring and Control Centre (MCC) Abu Dhabi requirements is mandatory.

PE 2.4 Ownership of Secure Areas [T]

Each Secure area should have a designated 'Owner' who is responsible for monitoring the security of that area.

The designated Owner:

a) should be responsible for quarterly monitoring of the records/logs and surveillance footage.

b) should also maintain an up-to-date list of users for the secure area, authorized by the management.

c) should also maintain an inventory of physical keys, cards or other access methods including current holder. This list should be kept confidential.

d) Should change the combinations and keys for any entity-defined secure zones, entry/exit points, and cabinets, when compromised.

PE 2.5 Protection against External & Environmental Threats [B] [S]

The entity should design and apply physical protection against natural disasters, environmental threats, external attacks and/or accidents. This should take into account how their healthcare delivery capacity maybe affected due to external and environmental threats. Large healthcare facilities should take into account their responsibility as care provider to surrounding areas facing a critical situation.

The entity should implement and maintain environmental control systems for data centers, that monitor, maintain, and test the consistency of temperature and humidity conditions in accordance with regulatory requirements and ensure appropriate fire suppression systems (e.g., sprinklers, fire extinguishers) are located throughout the entity, and are no more than 50 feet away from critical electrical components.

The entity should ensure fallback equipment, device, system, and backup media are protected from damage caused by natural or man-made disasters.

Generators and battery power backup should be available to provide power to key information systems and critical data center infrastructures.

The entity should also consider the external environment like fire in a neighboring building, water leaks etc.

PE 2.6 Delivery and Loading Areas [B]

Segregation of delivery and loading areas is a best practice to ensure control over incoming and outgoing materials. The method of implementation will depend on the size of the entity and the volume of materials handled.

Ideally, the external doors of a delivery and loading area should be secured when the internal doors are opened to prevent unauthorized access. All material should be inspected within this area and registered in accordance with entity's asset management procedures.

Access procedures for loading and unloading areas should be defined to restrict access only to authorized personnel and where applicable, physically segregate incoming and outgoing materials.

PE 3 Equipment Security

PE 3.1 Equipment Siting and Protection [B] [S]

The entity should site/position equipment and medical devices in manner that they are always protected.

Guidelines on physical protection and unauthorized access of equipment and medical devices should be established. When positioning equipment and medical devices, care should be taken to avoid the possibility of their exposure to high temperatures and humidity. Similarly, the entity should avoid placing critical equipment close to glass windows to avoid the risk from external incidents.

Equipment handling personal healthcare information with insufficient access control should be sited in a lockable area.

PE 3.2 Standard operating procedure for equipment [A] [S]

The entity shall establish operating procedures for commissioning, maintenance and decommissioning of equipment activities. These should meet or exceed the requirements and recommendations of the manufacturer. Equipment being decommissioned must be clear of PII and PHI

The entity should maintain up-to date records for maintenance carried out with information including but not limited to:

a) Date and time of maintenance

b) Name of individual performing maintenance

c) Name of escort

d) A description of maintenance performed and

e) A list of equipment removed or replaced.

PE 3.3 Cabling Security [B]

The entity shall protect equipment and medical devices from disruptions caused by failures in cables carrying power, telecommunication and cables carrying data.

a) Power, telecommunication, and cables carrying data should be protected in concealed conduits as far as possible to protect against physical tampering.

b) Power and telecommunication/data cables should be segregated to avoid interference. The entity should consider using redundant cables in difficult locations and in locations where a cable failure will have a high impact.

c) The entity should ensure controlled access to patch panels, cable rooms, and circuit breakers to prevent accidental or intentional misuse.

d) The entity should use electromagnetic shielding to protect cables from interference where applicable and should use fiber optic cables for data in areas with high electromagnetic radiation.

e) The entity should schedule physical inspections to identify deviations as well as unauthorized devices being attached to the cables.

PE 3.4 Security of Equipment Off Site [T] [S]

An entity's equipment, medical devices and information processing systems may be taken off-site for storage, maintenance or for remote working. Management should authorize taking equipment outside the entity's premises in any case.

In all situations, the entity should ensure security measures are applied to protect off-site equipment, medical devices, and information processing systems from the probabilities of information leakage, tampering and unauthorized activities.

In the case of storage or maintenance, the entity should ensure that no h Health Information is allowed to go off-site on the equipment. This is also applicable in case leased equipment being returned to a supplier.

The entity should ensure that the manufacturer's recommendation and instructions are followed, while equipment, medical devices and information processing systems are off-site, particularly the environmental conditions.

Movement and possession (chain of custody) logs for off-site equipment, medical devices and information processing systems should be maintained and verified, even if the possession goes outside the entity.

Any equipment and media taken off the premises should not be left unattended in public.

In the case of tele-working or tele-medicine, strong access controls and secure communications should be implemented. It is recommended to discourage access to Health Information from outside the entity's facilities.

PE 3.5 Clear Desk & Clear Screen Policy [B]

Information left visible on the screen or paper documents left unattended on the desk etc. form another method of information leakage. Similarly, removable storage drives, if allowed and when left unattended are also another source of data leakage.

If managed printing is not implemented by the entity, uncollected printouts left at the printer can be another source of information leakage as photocopiers. As such:

a) All unnecessary hard copies should be shredded before disposal.

b) All employees and contractors should be made aware of their responsibility.

c) In secure areas, contractors should not be allowed to use cameras or mobile phones when unsupervised.

d) Meeting rooms should be cleared of all confidential data at the end of a meeting. Health Information should not be left unattended anywhere.

e) The Clear Desk & Clear Screen Policy should be read and acknowledged by all employees and contractors of the entity

Domain 4 - Access Control

Access control processes enforce security requirements such as confidentiality, integrity, and availability of information assets to prevent unauthorized use of resources. Access controls shall be developed by entity to control access of employees, contractors and third-party users to entity's information assets and to manage their user access in reference to internal network, operating systems and, applications to and to ensure appropriate protection of entity's infrastructure.

Entities should take specific care when Health information is being accessed or used and should define access criteria that conforms to the following facts:

a) A healthcare relationship exists between the user and the data subject (the subject of care whose Health Information is being accessed),

b) The user is carrying out an activity on behalf of the data subject,

c) There is a need for specific data to support care delivery or continuum of care.

The entity's management should be aware of the risk environment and outcomes of unauthorized access, as it will be accountable for all consequences and impacts on:

a) Abu Dhabi Government,

b) Abu Dhabi Healthcare-ecosystem or Health Sector,

c) Patients concerned, and

d) Entity itself

The objective of this domain's controls are:

To ensure access to information and information systems are controlled, and to minimize probabilities of information leakage/compromise, tampering, loss and system compromises.

AC 1 Access Control Policy

AC 1.1 Access Control Policy [B]

The entity should develop, enforce and maintain an access control policy to ensure access to information and information systems are adequately controlled and secured.

The access control policy should consider all health information as confidential. While the importance of particular data may vary over time for each patient, the healthcare facility and their staff should treat all healthcare information as confidential at all times.

The access control policy should take into account the risks of working with mobile computing equipment in unprotected environments. The mobile related requirements should include physical protection, access controls, cryptographic techniques, backups, and virus protection.

Management along with designated asset 'Owners' should determine appropriate access rules and restrictions for specific user roles towards their assets. Users should have clarity on the information security requirements to be met by access controls.
When using mobile devices, e.g., notebooks, palmtops, laptops, smart cards, and mobile phones, special care should be taken to ensure that entity information is not compromised. This policy should also include rules and advice on connecting mobile devices to networks and guidance on the use of these facilities in public places.

The policy should:

a) Be relevant and appropriate to control and secure access to information, application, technology, medical devices and equipment;

b) Include management demands and directions, scope and specific applicability based on:

- Type of service,
- Information,
- Application,
- Technology,
- Medical devices and equipment.

c) Emphasize the requirement-of-need and role-based access principles.

d) Establish requirements, with core focus on:

- granting of access,
- access authorization,
- access revocation,
- access review.

e) Address the entity needs on secure password management and practices.

f) Mandate the usage of unique identity and complex password.

g) Where relevant, define control measures and provisions for portable/mobile devices, including user owned devices, that handle the entity's data or has the entity application(s) to conduct business transactions;

h) Include control requirements for the access and use of network services;

i) Include management actions on violations and deviations;

j) Define roles and responsibilities for actions expected.

Depending on the size and structure of the entity, the Access Control policy can be included as part of a single general information security policy document or can be split up into multiple policies that reflect the complex nature of the entity.

To facilitate entity policy development process, the DoH has provided sample Baseline Policies in Section 3 of this document. Entities are free to customize the provided baseline policies as per their environment as long as they remain compliant with the requirements of the ADHICS Standard and any other DoH or legal requirements.

Supporting or dependent entity policy references:

1. Physical and Environmental Security Policy
2. Clear Desk and Clear Screen Policy
3. Log Management Policy
4. Password Management Policy
5. Cloud Security Policy
6. Data Privacy Policy

The level of applicability of above-mentioned policies will vary depending on the individual entity.

AC 2 User Access Management

AC 2.1 User Registration and De-Registration [B] [S]

The healthcare entity should create unique user accounts with unique identifiers (user IDs) for each individual requiring access. The entity must establish measures to enforce the prohibition on sharing a single account among multiple users. Also, it is best practice not to reuse a user's ID even after the user leaves the organization. This is to ensure a departed user's activity can be traced if required.

A shared or group account should not be provided to users. Role-based access control can be implemented using groups and adding individual users to the groups as per approval. In this way the group memberships of a user will determine his access to systems in a controlled and auditable manner. Any deviation from this should be authorized and documented.

Credential sharing between staff should not be allowed. This has to be part of awareness training. Timely provision of required access to users will reduce the likelihood of credential sharing. It should not be acceptable for a new employee to be allowed temporary system access using another employee's credentials while their own credentials are being set up. This is a major violation and can have serious repercussions for the entity's information security. The right way to onboard a new employee quickly is to have a clear process in place between HR, IT and any other concerned department to optimize the workflow for onboarding employees. The entity should avoid incomplete data at each stage, whether personal information or access requirements to prevent delays in the process. A sample form is available in Section 5 – Forms.

If contractual or third-party workers have to be provided access, the same requirement of unique user account per user should be met. Additionally, an expiry date for the account is mandatory. The expiry date may be set based on the work requirement or contract duration. If no date is defined, then a default validity of 90 days can be used.

For all categories of users, the access granted to information systems and medical systems should be based on documented approval of the system's 'Owner'. Please refer to AM 2.3 of the Domain 2, Asset Management. Additionally, the entity's management approval may also be required in particular situations.

The employee Exit and Role Change Processes are covered in detail in Domain 1, Human Resources Security. Please refer to HR 4.1 to 4.4 for the relevant guidelines

The effective implementation of the above requires an up-to-date auditable record of persons authorized to use entity's information systems, applications, medical devices and equipment. Identifying and disabling or deleting inactive accounts should also be conducted on a quarterly basis In order to maintain proper accountability, it is important to ensure that all user activities are logged along with their respective identifiers

AC 2.2 Privilege Management [T] [S]

The entity should restrict and control allocation of privileges, based on principles of need to know.

It is a common mistake that normal user accounts are given enhanced rights to run as service accounts or to conduct system level activities. Even if the user is authorized for these privileges, separate

administrative accounts should be used for these activities to reduce the risk if the normal user account is compromised, for example by a phishing attack.

In the context of an entity, unauthorized modification or misuse or leaks of health Information is also a risk.

The entity should ensure that

a) Normal user accounts are not used as service accounts or used to conduct privileged application and system level activities;

b) “Privilege” or “Administrative” accounts are used by individuals with a role to conduct privilege activities;

c) Privilege user IDs are controlled and not shared with multiple users

d) Users privileges are restrictive in nature and are assigned based on needs to conduct business activities;

e) Privilege or administrative accounts are not to be used for conducting normal day to day operational activity;

f) Usage of service accounts are controlled and are not hardcoded in application codes or scripts;

g) There is multifactor authentication scheme for all administrative and remote access;

h) Mandated administrative or privilege access and associated activities are logged and audited.

AC 2.3 Use and Management of Security Credential [B] [S]

The entity should establish process for secure allocation, use and management of security credentials.

Default passwords are not to be used any context. All default passwords are to be changed before an application or system is put in use. Listings of default passwords are available on the internet and so provide no security at all.

Passwords should be stored encrypted. Plain text storage of passwords may expose entity to insider attacks as well as external. When a Username / password needs to be communicated to a user, it is not possible to encrypt the information. Therefore, the two should be sent in two different communications.

Password complexity and password history minimum current best practices are Twelve characters including one number, one upper-case and lower-case character, and a special character. Reusing the last three passwords should not be allowed. The entity should ensure passwords, including that of service accounts and privileged accounts are to be changed every 90 days. The entity should configure account lockout features to block the users after at least 5 failed attempts

User awareness training should educate users on selecting strong passwords that are easy to remember but difficult to guess. The entity can consider opting for alternative methods of authentication like Biometrics to improve access speeds in areas of critical healthcare delivery.

Users should be educated not to write down their passwords and not to utilize the password used on corporate systems for their personal accounts and vice versa. In the absence of Single Sign On, it is acceptable for a user to use the same strong password across multiple corporate systems.

AC 3 Equipment and Devices Access Control

AC 3.1 Access Control for Portable and Medical Devices [T] [S]

The entity should restrict access (role based and need based only) to on to portable or removable media, mobile or portable devices, and medical equipment or devices to protect confidential and secret information

Always protect data classified as confidential or secret. Use encryption on portable storage and mobile devices. Particular attention should be paid to medical equipment and devices as well as portable devices which may have weak or simple default passwords. Passwords for equipment and devices should follow password policies if it is not possible to use single sign on.

AC 3.2 Access Control for Assets and Equipment in Teleworking Sites [T] [S]

The entity should control access to equipment, devices, system and facilities at teleworking sites.

Teleworking introduces a set of information security risks which have to be mitigated by the entity. Physical security at the teleworking site should be assured to protect the teleworking equipment as well as possible misuse of the connectivity to corporate networks. External access to resources can also be made more restricted, only allowing access to required resources.

Authentication should be required for all remote access to entity information assets. Access should be only for authorized users.

The entity should ensure confidentiality and protection of information during the transmission Health Information while providing/consuming services through teleworking principles, including telehealth related services.

Random audits should be conducted of the equipment and facilities at the teleworking sites. The entity should maintain an up-to-date asset inventory for teleworking sites with designated 'Owners' taking responsibility of the equipment even when not in use.

Users should be made aware of the risks of equipment and data loss. Up to date anti-malware software should be present. The communications link should use the current best practice encryption protocols. Virtual desktop solutions can be considered to minimize data leakage.

AC 3.3 Telehealth Security [B] [S]

The biggest problem with telehealth is that it decentralizes the entity network. As new devices and applications are used in entity headquarters, in the cloud, and now at home, attackers have more potential entry points.

The entity is required to strictly adhere to the security and privacy requirements specified in the DoH standard for Telemedicine. Additionally, it must fully satisfy the requirements outlined in this standard when providing Telehealth services. When collaborating with third-party providers of telehealth services or equipment, the entity must ensure that these parties are compliant with both the DOH Standard on Telemedicine and the requirements of ADHICS

Healthcare entity should consider their policies for patient electronic communication, social media use, mobile device security, and acceptable technologies and applications (apps). Entities can identify risks associated and take action to resolve them with the use of a risk analysis that takes into account the services provided, the manner of delivery, and the types of technology used.

AC 4 Access Reviews

AC 4.1 Review of User Access Rights [B] [S]

The entity should review user access and associated privileges to various entity resources periodically

Access reviews should be conducted every three months for critical systems and at least once a year for others. The designated 'Owner' of the resource will confirm whether to discontinue or continue a particular user's access.

The owner should maintain a log of access and privilege requests along with the approvals. Access granted but not utilized should be revoked after the entity's defined period of inactivity. This is to prevent misuse.

AC 5 Network Access Control

AC 5.1 Access to Network and Network Services [B] [S]

Access to the entity's network and network services should be controlled and may be provided based on specific need for which the user is authorized for.

Network managers should implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. In particular, the following items should be considered:

a) Operational responsibility for networks should be separated from computer operations where appropriate.

b) Responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established

c) Special controls may be required to maintain the availability of the network services and computers connected

d) Management activities should be closely coordinated both to optimize the service to the entity and to ensure that controls are consistently applied across the information processing infrastructure.

Further measures can include:

a) Implementing ingress and egress filtering to allow only those ports and protocols with an explicit and documented business need

b) Restricting access only to trusted sites (whitelists)

c) Inspecting packets on DMZ networks using Security Event Information Management (SEIM) or log analytics systems

d) Deploying Sender Policy Framework (SPF) records in DNS and enabling receiver-side verification in mail servers

e) Disabling/uninstalling unused services

f) Enabling host-based firewalls or port filtering tools on end systems with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

g) Regularly scanning port on all key servers, and compare results to a known effective baseline.

h) Ensuring backup and protection of firewall, router, and switch configurations

i) Authorization and Multifactor authentication with Cryptographic techniques for remote access to entity systems

j) Providing access to shared and isolated networks in line with entity's Access Control Policy, requirements of business applications and need to access shared resources.

k) Controlling user access to shared and isolated networks. Using segregated networks allows granular control over access to different parts of the network. The connectivity allowed should be to areas relevant to the role of the user. Connection control can also be used to restrict traffic from individual users to the internet.

AC 5.2 Equipment Identification in Network [A]

The entity should identify all equipment and devices connected to its network and should have an automated mechanism to detect unauthorized equipment and devices.

The entity should ensure that only authorized devices are connected to its network. The controls used will depend on the size of the entity. Network Access Control (NAC) equipment can be used in larger entities whereas physical control could be used in small entities.

It may be necessary to consider physical protection of the equipment to maintain the security of the equipment.

AC 5.3 Remote Diagnostic and Configuration Protection [A]

The entity should control access to all information assets for the purpose of diagnostic and configuration. Medical equipment, computer systems, network systems, applications, communication systems etc. may have a remote diagnostic and configuration port for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access. Connectivity to these ports should be enabled only when required and with authorization.

Processes are created to regulate logical and physical access to the port, such as ensuring that diagnostic and configuration ports are only available by to authorized hardware/software support people The entity should:

a) Identify and whitelist all ports, services and utilities that are used for troubleshooting, and for diagnostics and configuration purposes.

b) Provides rationale or define security controls for the diagnostic and configuration services and utilities that are essential, and disable services and utilities that are not required.

c) Restrict access for remote troubleshooting, diagnostic and configuration to authorized roles and from authorized workstations.

AC 5.4 Network Routing Control [T] [S]

The entity should define and implement network routing controls to ensure information flow and system, devices, equipment connections are not compromised and are in line with requirements of Access Control Policy. Implementing routing control adds a layer of protection to entity network traffic. All traffic from an endpoint can be routed as required. This will reduce the lateral movement of malware if an endpoint is compromised.

Traffic from/to the DMZ should also use routing control.

The entity should:

a) Establish processes for secure configuration and rules application for network routing requirements.

b) Always ensure source and destination address and services or ports are used while defining and applying routing rules.

c) Enable routing protection countermeasures to avoid manipulation of routing systems and tables.

d) Implement network perimeters to ensure that all outgoing network traffic is routed via them. Internet traffic should go via at least one application layer filtering proxy server.

e) Define and implement network architecture that segregates and isolates internal and publicly accessible systems.

f) Manage External connections to information systems and networks outside the entity through interfaces consisting of perimeter protection devices (such as firewalls).

g) Ensure that communications with external systems, networks and key internal systems are always monitored for malicious and suspicious payloads.

h) Review and update the configured rules, as required

i) Periodically scan for any covert channel connections to public networks bypassing entity security defense.

AC 5.5 Wireless Access [T]

In a wireless environment, there are potential vulnerabilities that attackers can exploit, such as intercepting wireless signals, gaining access to wireless networks, and stealing sensitive data. Thus, The entity shall ensure wireless access within the entity is secured.

Use of wireless connectivity to internal networks is not recommended. If imperative, then wireless controller-based access using verified endpoints and entity's internal authentication scheme can be used. Privileged and administrative accounts should not be used over unsecured Wi-Fi. Disable Bluetooth, Wi-Fi and other wireless technologies on medical equipment and devices unless it is being used.

The entity should:

a) Establish usage restrictions and secure configuration requirements.

b) Establish authorization process for wireless access and usage.

c) Ensure only trusted devices and users gain access to internal networks via wireless access.

d) 4Ensure that internal wireless is not broadcasted.

AC 6 Operating System Access Control

AC 6.1 Secure Log-On Procedures [B] [S]

The entity should establish and enforce secure log-on and log-off procedures to control access to system and applications, medical devices. The secure log-on and log-off procedures will:

a) Limit the number of unsuccessful log-on attempts

b) Enforce recording unsuccessful and successful attempts

c) Control further wrong attempts without specific authorization from an administrator

d) Control displaying the password being entered by hiding the password characters with symbols

The entity should:

a) Ensure that access to entities systems, applications and services that process, use or store Health Information are authenticated.

b) Enforce automated locking of workstation/system after a predefined period of inactivity and/or after consecutive unsuccessful login attempts

c) Automatically terminate inactive sessions after a predefined period of session inactivity.

d) Display a logon banner that requires the user to acknowledge and accept security terms and their responsibilities before access to the system is granted.

AC 6.2 User Identification and Authentication [B] [S]

The healthcare entity should create unique identifier (user ID) for each user who require access to entities systems, applications or services, and should implement a suitable authentication technique.

Unique user accounts are mandatory except in equipment that do not support multiple user accounts. It is best practice not to reuse a user id even after the user leaves the organization. This is to ensure a departed user's activity can be traced if required.

A shared or group account should not be provided to users. Role based access control can be implemented using groups and adding individual users to the groups as per approval. In this way the group memberships of a user will determine his access to systems in a controlled and auditable manner. Any deviation from this should be authorized and documented.

See also AC 2.1

AC_6.2 Use of System Utilities [A]

The entity should restrict and control the use of utility programs and tools that might be capable of overriding system and application controls.

Default OS installations include various utilities for administration, troubleshooting etc.

Attackers and even malware can misuse these utilities to escalate privilege and gain access to restricted areas of the host machine.

Most such utilities do not have logging functionality, and this is another reason to restrict access.

The entity should:

a) Identify essential system utilities and tools and enforce appropriate controls for use

b) Provide access to system utilities and tools based on appropriate authorization

c) Maintain inventory of access to system utilities and tools

d) Monitor use of system utilities and tools

e) Ensure deletion of file system, file execution permission denial of, all unnecessary software-based utilities and system software

Domain 5 – Communications and Operations Management

Communications and Operations management aims to establish and/or strengthen entities processes and efforts to improve and enhance control environment. Entity shall have controls in place to ensure the safe operation of information processing equipment and the security of data while it is transmitted across networks

The domain addresses requirements including but not limited to, backup, security of network, electronic communication and monitoring to ensure protection against malicious code and spyware

Objective outcome of effective operations management includes, but is not limited to:

a) Improved security and reduce probabilities of compromise

b) Reduced errors

c) Controlled unauthorized activities

d) Controlled information exchange through formal exchange agreements

e) Regulated efforts

f) Increased efficiency

g) Reduced security incidents

<u>The objective of this domain's controls are:</u>

To ensure that activities concerning entities processes, support and maintenance of data, technology, and application and communication are controlled and carried out in a standardized and secured manner to reduce probabilities of errors and compromises, and to increase efficiency and security.

CO 1 Communications and Operations Management Policy

CO 1.1 Communications and Operations Management Policy [B]

The entity should develop, enforce and maintain secure communication and operations management policy or alternatively, two separate policies for Operations management and Communications

management, to ensure operational and communication activities concerning data, technology and application are controlled.

The policy should:

a) Be relevant and appropriate to the entity's operational and risk environment concerning data, technology and application

b) Establish management demands on:

- Segregation of duties
- Configuration management
- Change management
- Baselines and minimum-security configurations
- Standard operating procedures
- Capacity management
- System acceptance
- Malware control
- Backup management
- Network Security Management
- Secure exchange of Information
- Electronic Commerce Services
- Logging and monitoring
- Patch management

c) Provide framework for managing operational activities

Depending on the size and structure of the entity, the Operations Management policy can be included as part of a single general information security policy document or can be split up into multiple policies that reflect the complex nature of the entity.

To facilitate entity policy development process, the DoH has provided sample Baseline Policies in Section 3 of this document. Entities are free to customize the provided baseline policies as per their environment as long as they remain compliant with the requirements of the ADHICS Standard and any other DoH or legal requirements.

Note that, besides the Operations Management Policy, this domain has the following supporting or dependent entity policy references:

1. Change Management Policy
2. Capacity Management Policy
3. System Acceptance Policy
4. Patch Management Policy
5. Logging and Monitoring Policy
6. Backup Policy
7. Cloud Security Policy
8. Third Party Security Policy

CO 2 Operational Procedures and Responsibilities

CO 2.1 Baseline Configuration [T] [S]

The entity shall develop and enforce baseline and recommended configuration and system settings for hardening of common information technology products and applications, virtual machines, medical devices and equipment.

The entity, while developing baseline and recommended configuration setting, should consider:

a) Manufacturer's security recommendations – Default settings will prioritize ease of use over security. The entity should evaluate configurations from the perspective of securing all devices and equipment.

b) Requirements of this Standard – Any setting which conflicts with the ADHICS standard should be changed. Any deviations/exceptions should be approved and documented.

c) Industry best practices – A good starting point for common information technology products and applications is the Center for Internet Security (CIS) Benchmarks which is a free and globally accepted resource.

d) Risk mitigation strategies – Based on risks identified in the risk assessment.

e) Corrective and preventive actions – Mitigations based on audit, assessment and incident outcomes.

The entity should periodically review and update the information system's baseline configuration as required as a result of key security patches, upgrades, and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware and components)

CO 2.2 Documented Operating Procedure [A]

The entity should s operating procedures for all support, operational and maintenance activities of information systems and application, medical devices and equipment

This is to ensure consistency of all support, operational and maintenance activities across the entity. These standard operating procedures should be signed off by management.

All entity stakeholders and involved third party (if any) should be aware of and have access to the current version of the operating procedures.

The operating procedures should cover normal daily processes as well as exceptional situations requiring shutdowns or restarts of equipment. Support contact information can be included where relevant. The documents should also include up-to-date diagrams. The documentation should be reviewed on a schedule unless a major system change necessitates a review.

CO 2.3 Change Management [T]

The entity should control changes to information systems and application, medical devices and equipment

The Change Advisory Board (CAB) should have business and operations representatives. A record has to be kept of all decisions taken. All affected stakeholders should be informed once a change is approved. Roll back plan should also be communicated.

The entity should:

a) Establish a Change Advisory Board to authorize changes

b) Define and enforce a change management process that addresses the following elements:

- Identification and recording of significant changes
- Planning and testing of changes
- Assessment of potential impacts
- Formal approval procedure
- Communication of change to all relevant stakeholders
- Identification of stakeholders responsible for the “build, test, and implement” portion of the change

c) Roll-back plan to be utilized during unsuccessful changes

- Post implementation assessment
- Maintenance of previous version of software, code and configurations
- Maintenance of CMDB with updated Configuration Items
- Advance notification of changes to be made by third party(if any)

d) Define information systems and applications, medical devices and equipment that should be covered by the Change Management Process

e) Ensure all major changes to Information Systems and Applications should be tested before being rolled out into production. All significant changes must be identified and tested. Impact evaluation must include information security impacts.

The Change Advisory Board (CAB) should have business and operations representatives. The Change Advisory Board or designated individual must approve the move from test/development to production.

A record should be kept of all decisions taken. All affected stakeholders should be informed once a change is approved. Roll back plan should also be communicated.

CO 2.6 Separation of Test, Development and Operational Environment [T] [S]

The entity should identify and separate development, test, staging and operational environments

The level of separation between operational, test, and development environments that is necessary to prevent operational problems should be identified and appropriate controls implemented. No Confidential and/or PII and PHI must be used for testing purposes. The change management process of the entity should be followed.

The entity should:

a) Identify the appropriate level of protection between production, staging, test, and development environments

b) Document and apply clear processes for the transfer of data, information, code, configuration, software and systems between environments

c) Ensure as-is operational data, confidential data and/or PII and PHI is not used in test environment

d) Restrict usage/migration of test data into operational environment

e) Ensure to test the change in testing environment before rolling it out in production state

f) Prepare a rollback strategy

CO 3 Planning and Acceptance

CO 3.1 Capacity Management [A]

The entity should identify and document current and future capacity requirements while planning for new information systems, applications and cloud environment.

New implementations should consider the technical possibilities for upgrading system resources including availability of parts during the lifetime of the system. Monitoring and measuring the capacity of information systems is critical to ensure availability of

healthcare delivery. Systems running low on resources like processing power, storage, memory or bandwidth will be slow and unreliable. Monitoring trends and having defined capacity thresholds is recommended to ensure capacity demands are addressed proactively. Long delivery and implementation times should also be taken into account.

Another side of capacity management is recovering inefficiently used capacity. This includes decommissioning of unused systems, database optimization and data archiving.

CO 3.2 System Acceptance and Testing [T] [S]

The entity should establish acceptance criteria for new information systems and applications, changes, upgrades and releases, in addition to satisfactory test results
The entity should:

a) Establish processes for system acceptance and ensure system acceptance is acknowledged by the relevant authoritative individual. All steps should be documented.

b) Develop test cases for each of the requirements and changes and ensure tests are carried out and test results documented prior to usage in an operational environment

c) Ensure production data is sanitized/masked prior to use for testing.

d) Ensure testing is never performed on production systems. PII and PHI should not be used for testing on development systems. Only dummy PII and PHI may be used.

e) Ensure user profiles (with permissions appropriate for the tasks) used for testing are different from the ones used for operational and development activities

f) Ensure development tools and/or editors are not installed on operational systems. Development tools allow modification of code and data and introduce a risk of unauthorized modification of both if present on production systems.

g) Ensure test data and accounts are removed completely before the application is moved into production state

The evaluation should include a review of the information security of the new system as well as its impact on the overall security of the entity's information systems.

CO 4 Malware Protection

CO 4.1 Controls Against Malware [T] [S]

The entity should implement security measures to prevent and detect malware in order to safeguard information assets

User awareness training along with anti-virus and anti-malware on all endpoints are basic security requirements. Centrally managing endpoint security will allow administrators to ensure endpoints are up to date and keep track of detections at the endpoint.

Best practice for end points is to have real time scanning enabled and immediate scan when removable media is inserted.

The entity should:

a) Ensure minimum security configurations is maintained in all information assets, as applicable and as relevant

b) Implement anti-malware and anti-virus protection mechanisms for network and individual information systems (server, workstation, mobile/portable computing devices, virtual machine, cloud environment, hard drives, USB devices etc.)

c) Ensure anti-malware and anti-virus protections mechanisms are updated and current. Also, make sure end users are not having an option to stop/modify the services of Antivirus/Antimalware solutions.

d) Prevent access to malicious websites or sites

e) Enable real-time protection capabilities

f) Establish and enforce periodic scan schedules

g) Scan removable media for viruses and malware on all occasions when they are connected to information systems

h) Disable auto-run features for removable media on information systems

i) 89. Disallow the use or installation of unauthorized software

j) Configure anti-malware and anti-virus protection systems to alert responsible stakeholders on event, incident or anomaly detection

k) Collect information about new threats and Provide ongoing awareness for users on techniques, tactics and procedure to avoid and minimize probabilities of malware and virus attacks

CO 4.2 Gateway Level Protection for Malware [A]

The entity should deploy gateway level protection mechanisms to detect and defend against malware and viruses

Email and Browser based attacks are currently the most common methods used to compromise endpoints. All such traffic should be scanned for malware and phishing attacks. Doing it at the gateway level gives protection before the attack reaches the endpoint as well as a central view of incoming and outgoing traffic. The gateway can block malicious sites as well as prohibited sites. For example, this functionality can be leveraged for a data leakage prevention functionality to block cloud-based storage like Dropbox etc.

The entity should implement network-based malware direction solutions where the server software provider specifically advises against installing host-based anti-virus and anti-malware.

The entity should:

a) Implement Email Authentication Solution to block harmful or fraudulent uses of email such as phishing and spam

b) Check any attachments or downloads from email and instant messaging for malware, before use

CO 5 Backup and Archival

CO 5.1 Backup Management [B] [S]

The entity should maintain backup copies of essential information and software needed to support care deliver and its operations

Backups are a basic requirement for a business. The sizing and technology chosen should be based on the entity data volume as well as the restore point and time requirements.

The entity should:

a) Establish backup management process that identifies;
    - Essential and critical information in support of care delivery, business and entity operations
    - Data owner
    - Data recovery point and time requirements
    - Backup frequencies, time of execution and methods
    - Security controls to prevent compromise of backup data
    - Data backup restoration frequencies and test criteria
b) Perform backup of all identified information assets and its critical data including the configuration
c) Establish a data restoration process that includes, but not limited to:
    - Obtaining management approval for performing restoration
    - Determining the time and date of the lost data
    - Determining the appropriate backup media/location to restore the data
    - Copying backup data from secondary storage and restoring it to its primary location or a new location using backup/restore software
    - Recording any error during the restoration process
    - Completing restoration of the appropriate data
    - Evaluating the integrity of the restored data
d) Ensure data backups are tested for restoration in accordance with the entity's defined recovery plan
e) Ensure data restoration requirements for continuity and recovery are adequately met
f) Ensure data backup of specific instances are not mixed, accidently or deliberately
g) Ensure backups are not stored on entity live environment

The entity should implement security controls to ensure backup data is secure and protected from unauthorized access, theft, and tampering. The entity should store backups on different medium away from live environment and/or at a secure remote location and away from the primary site, as applicable in line with the risk.

These controls include but not limited to:

a) **Encryption:** Backup should be restricted both in transit and at rest

b) **Access Controls:** Access of backups shall be restricted to authorized personnel

c) **Physical Security:** Backup media/tapes shall be stored in secured, fireproof, locked cabinets

d) **Restoration Testing:** Regular testing and restoration to check for recoverability of backups

CO 5.2 Archival Requirements [A] [S]

The entity should establish data archival requirements that satisfies entities retention demands and demands based on the applicable regulations and laws.

The entity should:

a) Establish formal processes for archival and destruction of data

b) Identify data-sets and establish retention requirements as needed by law, regulation, and entity demands

c) Identify and enforce archival criteria (what and when to archive, how long to archive) and methods (physical/electronic) that satisfies established retention timelines

d) Preserve data during archival

e) Destroy data that has crossed retention timelines and are no longer required by the entity

f) Maintain adequate record on archival and destruction

CO 6 Logging and Monitoring

CO 6.1 Logging and Monitoring Procedures [A] [S]

The entity should establish and enforce monitoring procedures for information systems and application, cloud environment, medical devices and equipment
Logging and Monitoring standard activities to build a normal pattern of activity will help identify a variation which needs to be investigated.

Logging and Monitoring procedures should:

a) Identify aspects (system use, administrator, privileges, operator and user activities, logon attempts, network, system and application traffic, security events, changes, internal processing, exception, information exchange, integration, access, backup process etc.) to be monitored

b) Define minimum time requirements for maintaining information gathered from monitoring activities

c) Define criteria for alerting and escalation

d) Have defined criteria that quantifies specific outcomes of monitoring as incidents

e) Establish roles for monitoring activities and assign specific responsibilities

f) Have measures in place to communicate alerts to relevant stakeholders to address the issues and enhance monitoring capabilities.

The entity should:

a) Identify minimum required information to be logged

b) Define minimum frequency requirements for reviewing each type of log

c) Define minimum time requirements for maintaining each type of log commensurate with legal, regulatory and entity demands

d) Ensure that logs are not tampered with or modified or destroyed

e) Ensure unauthorized access to logs are controlled

CO 6.2 Preservation of Log Information [A]

Operating systems and applications generate a large volume of logs on a continuous basis. The volume of the logs and distribution of the logs across systems means that they are not meaningfully utilized.

A secure centralized log management system will help with system utilization and performance trends, tracking deviations from entity policy and procedures, access control variances and violations as well as any potential sign of security breach or attack.

A Security information and event management (SIEM) system can collect, and aggregate log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. The software then identifies and categorizes incidents and events, as well as analyzes them.

Log retention period and archiving where applicable should be defined. The storage capacity requirements should be taken into account. Maximum integrity of the logs can be achieved if it is not managed by the individuals managing the information systems. (Segregation of roles and responsibilities).

The entity should preserve logs in a centralized log management system and have mechanisms in place to correlate the logs to identify any security threats or malicious activity

The entity should:

a) Control access to the centralized log management solution

b) Ensure the centralized log management solution is managed by individuals who do not have operational role in implementing or maintain information systems or application

c) Ensure logs are correlated to identify any security threats or malicious activity

d) Retain logs for a period commensurate with legal, regulatory and entity demands on each type of log

e) Define use cases and dashboards based on the entity's needs and industry recommendations, and should consider:

- System utilization and performance trends
- Deviation from entity policy and procedures
- Access control variances and violations
- Any potential sign of security breach or attack

CO 6.3 Clock Synchronization [B]

The entity should synchronize clock of all information systems with an agreed time source. An internal time source or an internet time server can be utilized.

Having all system times in sync is important in many situations. From an information security point of view, correctly tracing the sequence of events requires corelating log data across systems and synchronized clocks is critical.

The date/time format should also be standardized. Otherwise, the timestamp information can be misunderstood within applications as well as when overwriting or deleting old files.

The clocks of medical devices and equipment should be set the same as that of the connected systems. Regularly check that the clocks of all relevant information processing systems are synchronized. This is required as some device clocks tend to drift with time.

CO 6.4 Information Leakage [T] [S]

The entity should monitor information processing systems to prevent opportunities for information leakage

The first step is to instill awareness on users about information security and the necessity to keep all data secure unless classified as public. Classification of data is also a prerequisite for successful implementation of DLP.

Information leakage can be over the network, via USB storage devices or hard copies. Print management solutions help keep track over the printouts generated per user. Access to USB storage devices can be restricted by different methods. Central DLP software will give granular control per user. Network data leaks can be over email, cloud-based storage etc. Blocking firewalls, proxies, DLP software are options to secure this.

CM 7 Security Assessment and Vulnerability Management

CO 7.1 Technical Vulnerability Assessment and Penetration Testing [A] [S]

This control specifies the requirement of an independent vulnerability assessment and penetration testing (internal/external) of the entity's critical applications, infrastructure, systems, medical devices and equipment. This is to be done annually or in case of major changes or addition of a new system / application, a fresh scan may be required.

To confirm actual risks, penetration testing should be done following vulnerability assessment. Penetration testing will involve employing automated and manual testing tools and scripts to exploit vulnerabilities. Both internally and externally conducted penetration tests are acceptable. After manually confirming the data from the tests, the entity should create a mitigation strategy to safeguard the network and prevent access to the information.

Due to the sensitivity of the contents of this report it has to be classified as secret and stored with the highest security. The identified findings and vulnerabilities and the status of mitigation has to be shared with the entity's management periodically. Entity should periodically follow up on the progress and status of mitigation measures with the appropriate stakeholders/owners and verify the effectiveness and efficiency of mitigation measures by performing revalidation testing.

CO 7.2 Security of Assessment Data [A] [S]

A third-party contractor typically conducts the vulnerability assessment. As part of the vulnerability assessment a current and complete inventory of assets including network infrastructure, applications and internet facing devices will be provided to the service provider. At the end of the vulnerability assessment, the service provider staff will have up to date information on any weaknesses in the entity infrastructure.

This control specifies the actions required to reduce the security risk introduced by using a third-party contractor for the vulnerability assessment.

The entity should ensure that assessment data is not available with third parties engaged to conduct assessments beyond the time of engagement

The entity should:

a) Ensure that system, network, applications and security related information is shared with third parties when they are on-site

b) Ensure that all information related to the entity's system, network, applications and security infrastructures and environment and assessment outcomes are erased from the involved third party's assets and environment after the completion of the assessment activity

c) Ensure that any shared reports are suitably protected and controlled

CO 8 Patch Management

CO 8.1 Patch Management Procedure [B] [S]

The entity should define and establish formal procedure for updating and patching of information system and application, medical devices and equipment.

Vulnerabilities are regularly identified in any hardware or software with network connectivity. These vulnerabilities are then patched with software updates and/or firmware updates.

Patches are given three levels of criticality. Depending on the criticality a deadline for rollout should be defined. Testing of patches on a small subset is recommended.

The entity should:

a) Restrict the usage of obsolete software/technology/medical devices/ equipment

b) Ensure all systems and devices that process or communicate information are timely patched and protected

c) Define criteria and process for application of standard, urgent and critical patches

d) Ensure all critical security patches are applied as soon as practicable from the date of release.

e) Ensure patches are deployed to a subset of systems or devices to allow testing before deployment to all.

f) Ensure firmware on devices are kept updated

g) Ensure third parties provide advance notification to entity prior to the release of any patches or updates to the offered product or service

h) Periodically validate patch status of systems and devices in use

i) Ensure security patches and updates are obtained from trusted sources and are periodically implemented

CO 8.2 Tracking of Patches [A]

The entity should have mechanisms in place for effective tracking of patches to:

a) Ensure software and systems are up-to-date with the latest security patches. By tracking and installing security patches in a timely manner, entity can reduce the risk of your system being compromised

b) Install software updates and patches that sometimes cause compatibility issues with other software or hardware

c) Identify areas of inefficiency and make improvements to streamline the process. This can save time and resources and help ensure that patches are deployed in a timely and effective manner.

Automated patch management systems are recommended for larger organizations, dependent on their risk environment

CO 9 Information Exchange

CO 9.1 Information Exchange Procedures [T]

The entity should develop, enforce and maintain formal procedures on information exchange and transfer incorporating control measure that protects information during information exchange and transfer.

The risk of compromise is high when information is being transferred. Formal procedures are required defining the control measures to mitigate this risk. The procedure should take into account the classification and value of information. PII and PHI should always be provided the highest levels of protection.

The stakeholders and the authorizations required should be defined. Responsibilities and sanctions should be defined as part of the procedure.

The procedures should:

a) Include control measures to protect information from interception, unauthorized access, copying, modification, misrouting, destruction and reduce probabilities of compromise during information exchange and transfer taking into account:
    - Classification and value of information
    - Information exchange and processing environment
    - Stakeholders involved

b) Identify minimum technical standards for secure packaging and transmission of Health Information

c) Establish responsibilities and sanctions for actions and deviations

d) Define actions to be taken during issues, incidents and deviations

CO 9.2 Secure Practices for Information Exchange [B] [S]

The entity should develop secure practices and capabilities while sharing information.

The confidentiality and integrity of transmitted information has to be maintained. This is applicable to data transmitted internally as well as externally.

Accuracy of the data is critical in the context of healthcare delivery where misinterpreted data can result in a risk to the patient. Secure methods should be used within custom developed software to transfer information. Using interoperability standards are one way. Transmission methods should use error detection and fault handling besides encryption.

The entity should:

a) Maintain chain of custody for information while in transit.

b) Ensure secure integration of Electronic Medical Records (EMR) platform to Abu Dhabi Health Information Exchange Platform (Malaffi)

c) Connectivity with DoH (AD Healthcare Net) and provide all required information

d) Ensure that entity resources are given access to Malaffi with the proper authorization and based on need-to-know basis

e) Ensure PII and PHI or its backup is not stored, processed or transferred outside UAE, except in cases where a valid exemption is issued by DoH

f) Ensure that employees of the entity and third-party users involved in service delivery fulfill their responsibilities and provide assistance from within the UAE, unless a valid exemption has been issued by the Department of Health (DoH)

g) Do not share identified or de-identified Health Information with third parties, data processors inclusive of counterparts and partners, unless authorized by Department of Health

h) Ensure that information exchanged between entities, and information sharing communities are protected

i) Ensure that user-name and password are communicated using two different communication channels (email and SMS-text, or email and phone, etc.)

j) Encrypt critical information before transferring and ensure sharing decryption key using a different communication channel

k) Ensure usage of appropriate interoperability standards for the exchange or transfer of information between systems and custom-developed applications9. Identify and implement security requirements for exchanging information and software with third parties

CO 9.3 Information Exchange Agreements [B] [S]

The entity should establish agreements between the entity and external parties for the secure exchange of information and software.

Any exchange of h Health Information shall be governed by DoH regulations. All PII and PHI generated by the healthcare provider is owned by the patient (Data subject) himself / herself. The entity should ensure the security of the information. This control defines the topics to be covered in the agreement with the external party. Health Information

The agreement should also specify what happens to shared data at the termination or expiry of the agreement.

The entity should, prior to the beginning of exchange of information and software:

a) Brief and agree with the external parties on all security requirements to be included in the agreement with regards to the criticality and classification of the information to be exchanged

b) Agree on the process of notifying sender of transmission, dispatch and receipt

c) Clearly define roles and responsibilities of each party to the agreement

d) Establish non-disclosure agreements for all disclosures

e) Agree on the expiration date of the agreement

f) Include in the agreement:

- Definitions of information to be protected
- Classification of information to be shared
- Security requirements to be considered for information protection

- Duration of agreement
- Process for notification of leakage or any incident
- Ownership for data protection
- Right to audit and monitor activities that involve Health Information and personally identifiable information
- Control requirements in handling the information in line with the defined asset management policy

CO 9.4 Physical Media in Transit [B] [S]

The entity should protect physical media containing information during transit. Any physical media containing sensitive information should be handled with extreme care. Movement of the media should be tracked and logged

By default, physical media in transit is at risk of theft, loss or accidental damage. Suitable mitigation should be done based on the classification of the information on the media.

The entity could use at least one of the following to protect physical media containing sensitive Health Information from unauthorized disclosure or modification while in transit:

a) Locked containers;

b) Tamper-evident packaging (which alerts to any attempt to gain access);

c) Hand delivery by authorized personnel;

d) Reliable courier services

The entity should:

a) Identify and ensure that physical media containing sensitive is classified and labelled in accordance with the established classification scheme

b) Ensure that physical media in transit containing sensitive information is protected against:

- Information disclosure or leakage

- Loss of information or media
- Modification
- Unauthorized access

c) Ensure that physical media in transit containing sensitive information is adequately tracked

d) Utilize trusted entity staff or courier service for transporting media

e) Ensure that media is controlled and disposed as per the relevant policy

CO 9.5 Restrict usage of Public Domain Email [B] [S]

The entity should restrict the usage of public domain email address for any official purposes and ensure that the data transmitted through those email accounts remains within the country's jurisdiction. This helps maintain data sovereignty and ensures that sensitive information is governed by local regulations.

CO 9.6 Electronic Messaging Protection [T]

The entity should protect information involved in electronic messaging. Electronic messaging is constantly evolving. Often, ease of use takes precedence over security for example in the case of filesharing sites. The entity should evaluate and only use approved technologies with suitable restrictions and controls implemented.

Transmission of healthcare information should be with the highest safeguards. Patient consent may be required.

The entity shall:

a) Identify and categorize all means of electronic messaging through which the entity information can be transmitted

b) Define specific control requirements for each identified category of electronic messaging

c) Ensure exchange of information is based on need and are addressed to authorized and legitimate resources

d) Ensure restrictions are implemented regarding forwarding of communications (e.g., automatic forwarding of electronic mail to external mail addresses), as applicable

e) Restrict the usage of public domain email address for any official purposes

f) Ensure appropriate electronic signatures containing legal disclaimers are used for electronic messaging

g) Educate employees about the best practices to be followed for electronic messaging

CO 9.7 Secure Transfer across Business Information System [A] [S]

The entity should develop, enforce and maintain procedures to secure information transferred across business information systems, EMR, Medical devices and equipment etc.

Vulnerabilities in the interconnections between systems should be addressed. There is a risk that information is accessible to unauthorized staff, or that encrypted data is decrypted during this process.

Connections between proprietary healthcare networks and entity administrative networks should also be evaluated for security.

The procedures shall:

a) Identify all points of interconnections and integrations between business information systems and identify the information to be protected

b) Identify adequate security measures to be applied to protect each type of information

c) Implement strong encryption capabilities for secure data exchange between medical devices and equipment, as applicable

d) Ensure integration of any medical device, solution and technology with EMR system and/or any critical infrastructure is protected by adequate measures such as encryption, secure protocols, dedicated physical connection etc.

CO 10 Electronic Commerce

CO 10.1 Security of Electronic Commerce Services [T] [S]

The entity should protect electronic commerce service and information involved passing over public and untrusted networks from service compromise and fraudulent activity, contract dispute, unauthorized disclosure and modification.

Entities which use websites or mobile applications for ecommerce or online transactions should identify and implement security measures to protect information online. Care should be taken that ecommerce data does not reveal personal Health Information as part of the billing. If they do, then additional steps to reduce the risk of compromise should be taken.

Ensure security requirements are agreed and captured in service agreements with electronic commerce partners and regularly monitored. An online presence will be targeted by malicious attackers and all partners have to ensure the security of their systems as well as the interconnections.

CO 10.2 Online Transaction [T] [S]

The entity should protect information involved in online transactions against incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure and unauthorized message duplication or replay.

Further to CM 10.1, the online financial transaction itself must be secure. The payment gateway and the entity should comply with all applicable laws and regulations. Always enable any optional security offered by card issuers

The entity should:

a) Identify all information used in online transactions

b) Identify and implement security measures to protect information used in online transactions

c) Ensure security requirements are agreed and captured in service agreements with partners involved in online transactions

CO 10.3 Publicly Available Information [A]

The entity should protect information available through the publicly accessible system. The entity should ensure that non- public information available is not available on publicly accessible information systems and systems are hosted in compliance with the applicable laws and regulations.

Entity information that is published, for example through websites or mobile application should have prior management approval. The process to be followed before information is made public should be documented. Information should be sanitized to remove any Health Information

Entity systems should enforce current industry standard encryption. Older cryptographic protocols should not be allowed as they can be compromised.

If end-user data is collected during online interaction, the information should be transmitted and stored securely at all times.

The entity should:

a) Identify all information available through the publicly accessible system

b) Establish process to publish and maintain information on the publicly accessible systems

c) Ensure information is sanitized and approved before publication

d) Ensure no healthcare and related data is exposed to the public domain

e) Define security measures to publish information on publicly accessible systems

f) Ensures that information available through the publicly accessible system is always available and is protected against unauthorized modification

g) Ensure non-public information is not available on publicly accessible information systems and systems are hosted in compliance with the applicable laws and regulations

CO 11 Information Sharing Platforms

CO 11.1 Connectivity to Information Sharing Platforms [A]

The entity should ensure that connectivity to information sharing platforms is secure and controlled.

Transfer of Health Information to sharing platforms is strictly regulated by the DoH based on legal mandates. Transfer of Health Information outside the UAE is normally not allowed unless exception to do so is granted by DoH.

Connectivity from every entity to Shafafiya (Medical Insurance) and Malaffi (Abu Dhabi Health Information Exchange) are mandated by DoH. Maintaining the security of the data and the connection is a shared responsibility.

The entity should:

a) Maintain a list of information sharing platforms that the entity connects to and/or operates

b) Determine security requirements for connecting to or release of information into identified information sharing platforms

c) Establish security requirement for accessing entity operated information sharing platforms

d) Develop required capabilities to establish secure connectivity to any required sector, national or international information sharing community

CO 12 Network Security Management

CO 12.1 Network Controls [B] [S]

The entity should ensure that all networks and supporting infrastructures are adequately managed, controlled and protected.

Besides listing and classifying network assets as part of asset management, entity networks and related infrastructure should be documented. Up to date network diagrams should be maintained showing the interconnections. Documentation should extend to patch panels and network wall sockets. The diagrams reviewed periodically and updated based on changes to the network

Current stable firmware should be in use. Configuration backups of network equipment (router, switches etc.) should be stored securely. Central management tools can help on large networks. Consider network access control to block unauthorized users on large networks. Internal firewalls between segments of large entity networks can help maintain security. Firewalls can control incoming and outgoing traffic on networks, with predetermined security rules. Firewalls can block malicious traffic, particularly Next Generation Firewalls, which concentrate on thwarting malware and application-layer attacks, are crucial to network security.

The entity should:

a) Ensure that all network components and interconnections are identified and sufficiently documented, including documentation of updates incorporated via the change management process

b) Ensure that network documentation includes up to date network architecture diagrams and configuration files of devices (e.g., routers, switches)3. Prohibit the use of insecure protocols like FTP, Telnet and use only secure protocols such as HTTPS, SFTP

c) Ensure information assets operate with only minimum needed TCP/UDP ports and disable all unused/vulnerable ports, services and protocols

d) Identify threats and vulnerabilities affecting network components and network as a whole

e) Implement specific security controls to mitigate identified vulnerabilities

f) Continually monitor implemented controls for their efficiency and effectiveness

CO 12.2 Segregation in Networks [T]

The entity should segregate physical, logical and wireless networks based on criticality, nature of services and users of the information systems.

Depending on the size of the entity and the complexity of its network topology, the entity should also implement segmentation (also known as network isolation) to divide network into multiple subnetworks in order to improve performance and security.

The segmentation should take into account the bandwidth demands as well as the value and classification of the information stored or passing through the segment.

Segmentation operates by controlling network traffic between the various components. The entity may decide to block all traffic from one area from reaching another or could choose to restrict the flow based on the type of traffic, the source, the destination, and a variety of other factors. Consider network access control to block unauthorized users on large networks. Internal firewalls between segments of large entity networks can help maintain security.

Medical imaging systems like the Picture archiving and communication system (PACS) or security CCTV systems may have very high bandwidth requirements that require a physically separate network.

The entity should:

a) Establish criteria for network segregation

b) Establish and maintain appropriate network security zones, allowing data flow follow through controlled path

c) Establish minimum and specific security requirements for each of the segregated networks, zones and resources

d) Ensure medical device and equipment network and Remote Patient Monitoring network is segregated from corporate network

e) Ensure medical device and equipment and Telehealth administration and management activities are conducted via a separate segregated network

f) Implement network segmentation and an access control policy to allow permitted traffic to selected network devices

g) Periodically evaluate the adequacy of implemented segregation strategy and identify areas of improvement

CO 12.3 Security of Wireless Networks [B]

The entity should ensure that all wireless networks are adequately protected.

The use of wireless networking for the entity's internal network is not recommended. Wireless internet access can be provided to guests and visitors, but the service should be provisioned on a completely separate network from the entity internal network. This guest network should have encryption and authentication enabled. Activity on the guest network should be logged.

A wireless network does not have a physical boundary. However, it is recommended to manage the location and power output of the Wi-Fi access points to ensure minimum leakage outside the entity premises.

For internal networks wired networks are always the preferred option and wireless networking should be used only if it is a necessity. Use of wireless networking introduces the possibility of Denial of Service (DoS) attacks as well as Man in the Middle (MitM) attacks which can affect the availability and confidentiality of data on the internal network. This is especially critical for medical devices and equipment. If wireless networks are used, then the strongest available authentication and encryption should be used. Use of unauthorized equipment like wireless extenders should be blocked and ensure public and guest access are segregated and isolated from the entity's internal network

Domain 6 - Data Privacy and Protection

Entities generate and utilize Personally Identifiable Information (PII) Protected Health Information (PHI)and establish relations with individuals to give the information a persistent value during its lifecycle of usage and references. Therefore, entity shall implement controls to prevent the inappropriate, unintentional, or illegal publication of any PII and PHI and to ensure that this standard is being followed.

Privacy of PII and PHI is a patient's basic right, by law and principles, and should be protected. Entities should demonstrate care, prudence and determination in protecting PII and PHI under their custody, and uphold the public trust placed on them.

PII and PHI is comprised of diverse range of data, including but not limited to:

a) Demographic data and general identifiers such as name, address, birth date, mobile number, Emirates ID etc.

b) Information that identifies the patient or for which there is a reasonable basis to believe that it can be used to identify the patient.

c) PII and PHI include information on the Patient's past, present or future physical or mental health condition and the provision of health care to the patient, or details of medical insurance.

d) Past, present, or future payment for the provision of health care to the patient.

e) Medical reports / records (Imaging and Lab reports, Prescriptions, Vaccinations record) whether it is in electronic or paper format.

f) Information about any organ donation to/by patient, of any body part or any bodily substance of that patient or derived from testing or examination of body part.

g) Genetic or sexual condition.

h) Family medical history.

i) Employee's compensation details, family members details, performance reviews, passport and National identifier details

j) Employment details, employee bank information, verification documents

The objectives of this domain's controls are:

To maintain privacy and ensure the security of PII and PHI in order to retain public confidence in the government's interests and values and to maintain entity reputation while providing healthcare services.

DP 1 Privacy and Protection Practices

DP 1.1 Data Privacy Policy [B][S]

The entity should develop, enforce and maintain a privacy policy that ensures management's commitment to protect PII and PHI collected and processed by the entity

This policy should be communicated to all persons involved in the processing of PII and PHI. Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management commitment.

Appropriate technical and organizational measures to protect personal healthcare information should be implemented.

The policy should:

a) Define management requirements on;

- Data Collection
- Data Collection
- Data Processing
- Data Security
- Data Localization
- Data Disclosure
- Data Retention
- Data Management

Note that, besides the Health Information Privacy Policy, this domain has the following supporting or dependent entity policy references:

1. Information Security Policy
2. Acceptable Usage Policy
3. Compliance Policy
4. Disciplinary Actions Policy

DP 1.2 Consent Collection [B] [S]

The entity should offer a way for data subject or the authorized representatives to give consent prior to any PII and PHI processing. Through the informed, and freely given consent, entity will make data subjects active participants in the decision-making process about the processing of their PII and PHI, unless otherwise constrained by laws and regulations.

The entity should ensure that consent is received in a way that is both informed and transparent and complies with all applicable legal requirements. A record of consent will be kept by the entity.

The entity should inform the data subject that they may withdraw the provided consent at any time during processing/delivery of services. Withdrawal must be as simple as consenting. Where applicable, the entity must additionally disclose how the data will be used for automated decision-making. The agreement must be tied to one or more clearly stated purposes, followed by thorough justification.

DP 1.3 Lawful, Fair and Transparent Processing Procedures [T] [S]

The entity should not do anything with the Health Information in breach of any laws. Entity should use PII and PHI in a way that is fair. This means entity shouldn't process the Health Information in a way that is unduly detrimental, unexpected or misleading to the data subjects.

It is important to think more broadly about how processing personal data impacts the interests of the data subjects and groups involved, in order to determine whether entity is processing PII and PHI fairly.

In order to ensure transparency, the entity could provide effective notice to data subjects regarding: its activities that impact privacy including, but not limited to, the collection, use, sharing, safeguarding, maintenance, and disposal of PII and PHI; authority for collecting PII and PHI; the PII and PHI collected, the purpose(s) for which it is collected and how it will be protected etc.

The entity should ensure that PII and PHI is not processed ever in a manner incompatible with the purpose and the PII and PHI remains accurate throughout lifecycle.

DP 1.4 Technical and Organizational Measures [B] [S]

The Entity should keep track of all PII and PHI stored and processed in order to secure it against loss or compromise. The entity must implement appropriate technical and organizational measures for maintaining security and privacy of PII and PHI throughout its lifecycle. The entity must ensure secure processing and storage of PII and PHI, avoid data breaches, and facilitate compliance with relevant data protection obligations.

Depending upon the size, complexity and risk environment, entity should implement security controls including, but not limited to:

a) **System controls:** User access measures (E.g.: Physical and Logical Access Controls, Network Security, Data Security, Data concealment etc.)

b) **Process controls:** Compliance to data classification policies, Data backup and Retention policy, Privacy by Design & Privacy by Default when designing / updating / changing products, services, business systems and processes, Compliance Audits etc.

c) **People controls:** Signing of Non-Disclosure Agreements (NDAs) and Data Processing Agreements (DPAs), Trainings, awareness, Employee background checks, and / or any other project specific requirements.

d) The entity should ensure that only people who are physically present in the UAE or who have a valid license to practice their profession there have access to systems and applications that contain protected health information. Also, entity shall not transfer health information and its copies in any form, whether encrypted, anonymized, deidentified, pseudonymized, etc., are not stored, processed, or transferred outside the UAE. Any exemptions must be approved by entity management and then submitted to the Department of Health (DoH) for further approval.

DP 1.5 Data Processing Inventory and Data Privacy Impact Assessment (DPIA) [A]

The **[Entity Name]** should prepare Data Processing Inventory to visualize, track, and analyze, how PII and PHI is created, collected, used, shared, and disposed across the entity.

The inventory should include fields including but not limited to;

a) Description of the categories of PII and PHI

b) Details about the data subject

c) Individuals authorized to access personal healthcare

d) Period, purpose, limitation and scope

e) Details about data exchange/transfer

f) Mechanism of transfer, deletion, modifying or processing

g) Data related to the cross-border movement, if any

h) Technical and organizational measures related to information security and processing operations

The entity should conduct DPIA before implementing or acquiring information technology that stores, process, or transfers PII and PHI and/or before initiating any processing activity if it is likely to result in high risks. Additionally, if the risks change over time or if there are substantial changes to the processing activity, a reassessment may be necessary.

DPIA should also be performed, if automated processing will affect the data subject legally, if processing is extensive and involves PII and PHI, or if extensive, systemic public area monitoring is taking place.

The assessment should at least contain;

a) a systematic description of the processing operations and the purposes of the processing

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes

c) the controls to address the risks, security measures and mechanisms to ensure the protection of PII and PHI

DP 1.6 Data Processors Security [B] [S]

The entity should only appoint a data processor/third party that has sufficient technical and organizational measures that fulfil the secure processing requirements and document the PHI protection requirements that PHI processors are required to meet within contracts, either directly or through reference to policies or another agreement. This will help to ensure that data processors provide adequate levels of privacy and protection.

The data processors are only permitted to process data pursuant to the instructions of the entity. The same legal obligations that apply to contracts or other agreements between the entity and the data processor also apply to agreements between the data processor and a subcontractor who manages PHI on data processor's behalf.

The entity should reserve the right to terminate the contract with the data processor if the entity determines that the Data Processor has violated a material term of the contract.

DP 1.7 Data Breach Management [B] [S]

The entity should notify and communicate interested parties if it discovers a breach of PII and PHI in hold of the entity. When the PII and PHI breach is likely to result in high risk to the data subjects, the healthcare entity must inform the data subject of the personal data breach in a clear and plain language.

The entity should:

a) Notify Abu Dhabi Health SOC about breach at the entity and/or the relevant third party/data processor within defined timeline predetermined timelines

b) Ensure the breach notification and further updates to DoH includes all the information as requested by DoH. This includes at minimum:

- Nature/Cause of the data breach;
- Approximate number of impacted records and data subjects;
- Consequences of the data breach;
- Measures taken to address the personal data breach, and the mitigation plan;

- Additional documents and/or information related to the personal data breach, and the remedial actions taken;
- Name and contact details of the data protection representative of the entity, where further information can be obtained from.

c) Adhere to the “Data Breach Notification” guidelines published by DoH

d) Complete and submit the "Data Breach Form" in addition to submitting incident notifications and updates. This form must be shared with the DoH within 72 hours of acknowledging the incident

e) Document all evidences pertaining to data breaches investigation and resolution and provide DoH with the requested information within 30 working days after the initial reporting

f) Ensure Notification to affected data subject includes clear and concise information about the breach and its potential impact. This information includes, but not limited to:

- Description of the breach
- Potential risks and impact of the breach
- Steps taken to mitigate the breach

g) Ensure processes are established and the controls are implemented to minimize the occurrence of data breaches

h) Entity management will take complete accountability in the event of any data breach involving the entity and their staff

DP 2 Appointment of Data Protection Officer

DP 2.1 Requirement for Appointing Data Protection Officer [A]

Depending upon the size, complexity of the entity and the risk environment, the entity should appoint a Data Protection Officer (DPO) responsible for entity’s Data privacy protection program. The DPO shall directly report to the highest level of management in the entity (such as a CEO).

The appointment of DPO appointment is based on qualifications, including expertise in federal and international data protection law and procedures and the ability to carry out assigned duties. The

creation and implementation of privacy policies and procedures are among the duties. Other duties include acting as the point of contact for all complaints regarding privacy and guiding managers, users, data processors and involved third parties on their individual privacy obligations and the procedures that must be followed.

The entity shall:

a) Ensure there is no conflict of interest between the officer and the tasks assigned

b) Ensure contact address of the data protection officer is well communicated to all data subjects

DP 3 Data Subject Rights

HI 3.1 Protection of data subject rights [T] [S]

The data subject has the right of obtaining information about their PII and PHI i.e., Type of processing, purpose of processing, sharing of data, security controls, breach management process etc. The entity should have mechanisms in place to fulfill data subject requests for Transferring, correction, deletion of PII and PHI as requested by the data subject.

The data subject has the right to be informed of the appropriate controls in relation to any PII and PHI transfer to a third country (subject to exception approval required from DoH).

Domain 7 – Cloud Security

To handle threats, technological risks, and protections for cloud environments, cloud security controls are crucial. They also give the knowledge required to make wise information technology decisions for their treatment.

Entity shall implement procedures, personnel, physical and technical controls to ensure security of cloud-based data, applications and infrastructure. By defending against threats and assisting in safe and secure cloud operations, the implementation of cloud security policies will reduce the impact of harmful attacks.

The objectives of this domain's controls are:

To ensure confidentiality, integrity and availability of IT applications, data, systems and network resources hosted in the cloud environment

CS 1 Cloud Security Policy

CS 1.1 Cloud Security Policy [B]

The entity should develop, enforce and maintain a Cloud Security Policy to ensure the confidentiality, integrity and availability of all IT applications, data, systems and network resources implemented in a cloud environment are secured. These controls will ensure access to cloud-based entity information systems is requested and granted, security of cloud-based systems and data is monitored and analyzed, violations of cloud security are addressed and mitigated, and changes to cloud security systems and procedures are requested, tested, approved and communicated.

The policy should:

a) Be relevant and appropriate to the entity's cloud security demands and applicable legal and regulatory compliance requirements

b) Demonstrate management commitment, objectives and directions

c) Establish a process that facilitates:

d) Selection of suitable cloud service provider and scope of cloud services usage

e) Identification of suitable information security requirements

f) Signing of Service Level Agreements (SLAs) and Non-Disclosure Agreements (NDAs)

g) Assignment of roles and responsibilities related to use and management of cloud services

h) Agreement on data retention, portability and destruction requirements

Note that, besides the Cloud Security Policy, this domain has the following supporting or dependent entity policy references:

1. Access Control Policy
2. Communications and Operations Management Policy
3. Incident Management Policy
4. Compliance Policy
5. Third Party Security Policy
6. Health Information Privacy Policy

CS 1.2 Cloud Security Controls [T] [S]

The entity should ensure cloud environment is physically hosted within UAE without any of the environments, infrastructures, or systems outside the country including backup and disaster recovery and Health Information stored in cloud is not extended for access, use or support by;

a) Any other entity/party in a multi-tenant environment.

b) Any entity/party that provides analytical services

c) any entity/party that provides remote support from outside UAE, except in cases where an exemption to do so is issued by DoH

Depending upon entity risk environment, the entity should ensure implementation of Cloud security controls, which includes policies, technologies to secure data, applications, and infrastructure that are integral to the usage of cloud computing.

The responsibility for ensuring cloud security are assigned and agreed depending upon the nature of cloud offerings:

a) **Private cloud:** Entity shall be responsible for all aspects of security for a private cloud because it is hosted in entity's own data center.

b) **Public:** In public clouds, such as Amazon Web Services (AWS®) or Microsoft Azure®, the cloud vendor owns the infrastructure, physical network and hypervisor. The entity is responsible for managing OS, apps, virtual network, access to their tenant environment/account, and the data.

c) **SaaS:** SaaS vendors/providers are primarily responsible for the security of their platform, including physical, infrastructure and application security. However, the security of the data is with the entity. Entity should implement controls to prevent data exfiltration, accidental exposure or malware insertion.

The entity should identify security requirements and ensure implementation of controls including but not limited to:

a) Secure protocols, industry standard encryption for protection of data at rest, transit & processing

b) Logical segregation, access control and logging and monitoring of activities

c) Controls for change management assuring adherence to the entity's change management policy

d) Physical security and environmental controls for natural disasters, malicious attack or accidents

e) Identification of misconfigurations and vulnerabilities on periodic basis

f) Data Backup, redundancy and recovery, based on business criticality and impact assessment

g) Ongoing maintenance, patching and upgrades, as required

h) Incident management and Forensics requirements

Domain 8 - Third Party Security

Operational efficiency, time to deliver and cost saving aspects compels entity management to utilize third party services or resources to complement service delivery. Involvement of third parties in the process of care delivery and associated areas are inevitable and needs stronger control measures to secure entity assets and information.

Entity management should be cognizant of the fact that a significant portion of privacy breaches originates with **[Entity Name]s** that contracted activities and services to third parties. Adequate due diligence to activities and services to be contracted, and a proactive identification and definition of control environment to secure privacy and information assets would minimize damages and benefit entities and the government. Entities that entrust access to third parties acknowledge and share responsibilities for the breaches.

An entity's management should be aware of the risk environment related to third party services and resources, establish a suitable framework for third party management and define a control environment that should:

a) Reduce probabilities of information leakage and loss

b) Secure information assets

c) Minimize unauthorized access and usage

d) Uphold organizational and governmental reputation

e) Ensure service continuity

<u>The objectives of this domain's controls are:</u>

To ensure third party services are controlled through suitable procedural obligations and contractual terms to secure privacy and protect information assets.

TP 1 Third Party Security Policy

TP 1.1 Third Party Security Policy [B][S]

The entity should develop, enforce and maintain a third-party security policy to facilitate implementation of the associated controls and to reduce probabilities of risk realization concerning third parties.

The policy should:

a) Be relevant and appropriate to the relationship of the entity and the third party

b) Establish a framework that facilitates:

- Secure management of third-party services and their role in healthcare and/or related services
- Defining and including information security objectives
- Third party briefing of security requirements
- Definition of roles and responsibilities

c) Demonstrate management's commitment, objectives and directions

d) Establish management's expectations on:

- Privacy and protection of information assets
- Access to system, application, device, equipment and critical area
- Nondisclosures and terms of use

e) Be read and acknowledged by stakeholders and third-party representatives authorized to sign on their behalf

Depending on the size and structure of the entity, the Third-Party Security policy can be included as part of a single general information security policy document or can be split up into multiple policies that reflect the complex nature of the entity.

To facilitate entity policy development process, the DoH has provided sample Baseline Policies in Section 3 of this document. Entities are free to customize the provided baseline policies as per their environment as long as they remain compliant with the requirements of the ADHICS Standard and any other DoH or legal requirements.

Note that, besides the Third-Party Security Policy, this domain has the following supporting or dependent entity policy references:

1. Access Control Policy
2. Operations Management Policy
3. Procurement Policy
4. Supply Chain Management Policy
5. Compliance Policy

TP 2 Third Party Service Delivery and Monitoring

TP 2.1 Third-Party Service Delivery Agreements [B] [S]

The entity should identify and enforce security requirements, service levels and management requirements as part of relevant third-party services agreements.

The entity should:

a) Ensure that specific security requirements essential for each of type of services are included in the service delivery agreement

b) Establish minimum security requirements for each identified service

c) Ensure measures and minimum baselines for each of the identified security requirements are established and monitored

d) Establish service levels for each of the service through third parties

e) Define and document the type of information that third party service provider needs access to

f) Assign responsibility for managing third party relationships to an individual or service management team

g) Identify and include Right-to-Audit terms specific to the provisions and environment of service management

h) Coordinate with entity contract management and legal teams for third party service requirements that needs the storing, processing and transmission of health and/or personally identifiable information

TP 2.2 Monitoring and Review of Third-Party Services [A]

The entity should monitor, and review services provided, and reports and records submitted by third parties. Third parties are used for operational efficiency, time to deliver and cost saving. However, third parties should be held accountable via contracts for timely delivery of services as well as for protecting any confidential data they store or process.

Unless the third party is directly involved in healthcare delivery, they should normally not have access to personal healthcare information.

Risks from third party administrative and cleaning staff are often ignored but they pose new challenges and threats to entities. The entity's management should apply adequate control measures to address those risks.

The entity should:

a) Monitor compliance of security requirements identified in agreements with third parties

b) Conduct security assessments and audits in accordance with this standard's applicable mandates and the entity's information security needs

c) Implement controls for authenticating and monitoring the exchange of information between various parties to ensure security compliance

d) Manage incidents and contingencies associated with access and violations

e) Assess and manage business, commercial, financial and legal risk associated with third party services

f) Perform audits of third parties' services on a regular basis

TP 2.3 Managing Changes to Third Party Services [T]

Changes may be required during the life of a contract. The entity should manage changes to the provisions of third-party services through a formal change management process. For every change planned, the relevant stakeholders should ensure that changes to activities and provisions are in compliance with security requirements. Any changes to entity policies and procedures should be intimated to the third-party vendor if relevant.

A formal change management process should be part of the agreement. Parameters of change should be communicated and agreed between the entity and the third party. If the third-party vendor itself is changed, ensure no sensitive entity data remains with the prior vendor.

Domain 9 - Information Systems Acquisition, Development, and Maintenance

The demand for systems and applications to host and process information to deliver business values needs careful assessment of lifecycle aspects. Wide options and cost-effective delivery models attract entities to determine easy to use and cost-effective solutions, ignoring security aspects in order to quickly deliver on business values.

Entity management should identify the relevant Health Information Health Information systems and applications, -related risk factors that impact the entities ability to provide reliable services, reputation and reliability of the solution/product or vendor. Entity management should be aware of the fact that the solution or the product selected will probably introduce new risks that should manage through their lifecycles.

Based on detailed assessment and entity risk appetite, the entity's management should choose from one of the below options:

a) In-house development, maintenance and support of application and systems

b) Outsource the development, maintenance and support of application and systems

c) Out-of-shelf product deployment, maintained and support by the vendor

d) Cloud-based application utilization

e) Hybrid approach for the development, maintenance and support requirements

Of these any cloud-based option is not acceptable when any personal healthcare information or other personally identifiable information is to be stored or processed. The DoH may permit limited use provided the cloud is proven to be fully hosted within the UAE. Storage of such data outside the country may be liable for penalties under Law No. 2 of 2019.

<u>The objectives of this domain's control are:</u>

To emphasis the need for entities to adopt secure system and software development lifecycle management processes and to ensure that systems and applications in use are securely managed and supported to avoid misuse of privileges and authority, reduce probabilities of information, system and

application compromises, and to uphold entity and Abu Dhabi government's reputational value and public trust.

SA 1 Information Systems Acquisition, Development, and Maintenance Policy

SA 1.1 Information Systems Acquisition, Development and Maintenance Policy [B]

The entity should develop, enforce and maintain an information systems acquisition, development and maintenance policy to facilitate implementation of secure development and maintenance practices.

The purpose of this policy is to ensure information security requirements are integrated into every part of the software lifecycle for entities.

The policy should:

a) Be relevant and appropriate to the model and relationship of the entity and involved internal and external stakeholders

b) Demonstrate management's commitment, objectives and directions

c) Establish a framework that facilitates:

- Defining and including information security objectives
- Selection of the right model and approach
- Identification and mitigation of risks in involved business and application processes
- Definition of roles and responsibilities

d) Establish management expectations on:

- Privacy and protection of information assets
- Secure design, development, testing, deployment, maintenance and support
- Secure access to systems, applications, devices, and equipment
- Secure processing and communication of information and data
- Non-disclosures requirements

e) Cryptographic controls and requirements

f) Be read and acknowledged by involved internal and external stakeholders

Depending on the size and structure of the entity, the Information Systems Acquisition, Development, and Maintenance policy can be included as part of a single general information security policy document or can be split up into multiple policies that reflect the complex nature of the entity.

To facilitate entity policy development process, the DoH has provided sample Baseline Policies in Section 3 of this document. Entities are free to customize the provided baseline policies as per their environment as long as they remain compliant with the requirements of the ADHICS Standard and any other DoH or legal requirements.

Note that, besides the Asset Management Policy, this domain has the following supporting or dependent entity policy references:

1. Access Control Policy
2. Operations Management Policy
3. Communications Policy
4. Procurement Policy
5. Third party security policy
6. Compliance Policy

SA 2 Security Requirement of Information Systems and Applications

SA 2.1 Security Requirements Analysis and Specification [T] [S]

The entity should analyze, identify, develop and implement information security requirements for new information systems and applications or enhancements to existing systems and applications.

Incorporating information security demands at the start is necessary to achieve a satisfactory result. The entity should take into account their own Risk assessment along with the demands from the sector regulator as well as any applicable laws. Information security must be considered whether the new system is developed in-house or bought off the shelf.

Technical system requirements are also to be verified as the availability and integrity of the system can be compromised if sufficient resources are not available. Information security enhancements like encryption may add to the system requirements.

The security requirement should:

a) Be relevant to be used for new information systems or enhancements to existing information systems

b) Be approved by individuals authorized to do so on behalf of business and information security

c) Address all risk elements identified during risk assessments throughout the system development lifecycle

d) Address risks from all software components, medical device and equipment

e) Consider additional/compensating controls if design level risk mitigations are not possible

f) Be compliant with the requirements of this standard and secure coding practices

g) Outline validation criteria to verify security control efficiency and effectiveness.

h) Ensure no activity in development lifecycle is carried out outside the boundaries of UAE

i) Define system acceptance criteria

j) Ensure maintenance of High-Level Design and low-level design of the System Architecture with descriptive details of every component in the architecture along with their interconnectivities

SA 2.2 Developer Training [A]

The entity should ensure developer of information systems, system components or information system services are provided suitable training prior to their involvement in development activities. The need to use qualified developers is obvious. This control emphasizes the need to ensure developers have the right knowledge or are provide the necessary training before they are involved on the project. The training can be in any form, but records should be maintained.

This requirement is applicable for internal as well as external development teams. Information security should be part of the training scope.

The entity should:

a) Identify baseline training requirements that are essential to the developer
b) Acknowledge that developer(s) received relevant baseline training prior to their involvement in development activities
c) Identify training requirements based on implemented security functions and features
d) Design and execute training programs to address additional and future security requirements
e) Include training requirement in agreements, when the requirements are delivered and managed by third parties

SA 2.3 Correct Processing in Applications [T] [S]

Due to the criticality of data that is handled in a healthcare facility, appropriate and adequate input validation controls shall be designed and incorporated into any operational or production application to the extent possible. By reducing the chances of erroneous data entry, we can improve the quality of healthcare delivery. Examples of validation can be out-of-range values, invalid characters, missing or incomplete data, duplicate records etc.

The entity should:

a) Define criteria, rules and validation parameters to validate data input into applications
b) Develop or configure applications to drop input data that is identified as incorrect or inappropriate
c) Validation checks should be incorporated into production applications to detect any corruption of information through processing errors or deliberate acts.

Validation of data should happen within program modules. Processing errors and system failures should not result in inaccurate or corrupted information. Programs processing in sequence should wait for the previous process to complete.

The entity should:

a) Establish minimum requirements for validation checks on internal processing of application under development to ensure correct processing of data

b) require application developers to provide evidence of compliance with minimum requirements

c) Ensure that the incorporated validation checks are valid and relevant over a period of time and meet minimum requirements through the applications' lifecycles

d) Requirements for authenticity and message integrity in applications shall be identified during the requirements phase of a project, and appropriate controls identified and implemented.

Integrity checks like hashes and digital signatures can be used. Some medical devices may also require special integrity considerations in relation to the electromagnetic emissions that occur during their operation.

The entity should:

a) Identify and enforce requirements to ensure authenticity and integrity of messages transmitted between systems and applications

b) Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances

In an entity, it is imperative that the patient identification and healthcare information retrieved is accurate. If there is a mismatch in the identification or the healthcare information, healthcare delivery will be severely compromised.

The output validation should be thorough, and a log of the validation should be maintained.

Additionally, it should be possible to identify incomplete data, especially in hard copies (missing pages).

SA 32.4 Off-line Processing Capabilities [T] [S]

The entity should ensure that all distributed and mobile applications are designed with the ability to tolerate communication failure. Mobile communications are prone to interruptions and applications should be able to recover.

For example, hash totals can be used to verify integrity.

Distributed and mobile applications should:

a) Include off-line and duplicate or out-of-sequence response message handling capabilities.

SA 3 Cryptographic Controls

SA 3.1 Cryptography and Key Management [T] [S]

The entity should establish key management to support the entity's use of cryptographic techniques and to secure cryptographic keys as appropriately.

Cryptographic keys are used to secure entity data and if compromised it could potentially expose confidential data. All cryptographic keys should be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store, and archive keys should be physically protected.

Entities should:

a) Establish process to:
   - Securely generate and use cryptographic keys
   - Securely share keys with authorized users
   - Protect keys against modification, loss and destruction
   - Set date of activation and deactivation for keys
   - Revoke/block keys
   - Repair damage or corrupted keys
   - Monitoring of key management related activities

b) Define standards for:
   - Key strength for various environments
   - Key storage

c) Protect secret and private keys against unauthorized use and disclosures

SA 4 Security of System Files

SA 4.1 Control of Operational Software [T] [S]

The entity should control the installation of software on operational systems
All software used within the entity should be controlled. Only approved versions should be used in production. Updates should be rolled out after testing. Versions no longer supported by the vendors can be a security risk and should not be used.

The change management process should be followed. Impact on healthcare delivery should be evaluated at all times.

If vendors are given access to systems or equipment, they should be monitored, and such access should be discontinued as soon as the installation is complete. Use of USB keys for updates should be monitored. Vendor USB drives should be approved by entity staff before use.

The entity should:

a) Ensure software installations are carried out only by authorized resources

b) Keep a copy of all software installed, including any previous versions

c) Adhere to software standards and ensure installation of only licensed software in an entity system

d) Ensures that no unauthorized software is installed on the system and maintain an up-to-date list of the authorized software that is necessary for the entity's various business purposes.

e) Ensure software installed in production systems are subject to entity change management process and approval

SA 4.2 Protection of System Test Data and Source Code [T] [S]

The entity should protect system test data and the source code

Protecting PII and PHI is of the highest importance. Any test environment does not need real PII and PHI. The use of dummy data should be preferred. Deidentified data and anonymized data can still be a risk. Sanitize test data from all systems. Keep a record of all test data.

Modified versions of custom developed programs can be created with unauthorized functionality if the source code is leaked. The entity should implement strict controls to protect the source code, with versioning to keep track of each production version.

The entity should:

a) Use sample data sets to test application, business and security functionalities

b) Restrict the use of real data from production systems for testing, allowing it based on appropriate control and authorization from authoritative business and information security stakeholders

c) Ensure PII and PHI is anonymized before making available for testing and training purpose

d) Ensure that access to program source code is strictly based on need and is in compliance with entity access control policy

e) Maintain records of copying, using and erasing of operational information in test environment

f) Ensure that personally identifiable information is not used as test data

g) Erase any data from test applications immediately after completion of the test

SA 5 Outsourced Software Development

SA 5.1 Outsourced Software Development [T] [S]

The entity should supervise and have control over outsourced software development.

Information security and secure coding should be core requirements. For continuity in case of vendor failure escrow arrangements should be made for the source code in cases where the entity does not have ownership of the source code.

No personal health information should be provided to the developer for testing.

The entity should:

a) Establish and enforce a secure coding policy

b) Define quality assurance processes

c) Include in the outsourced software development agreement the requirement to comply with:

- All relevant entity policies, including information security and quality related policies, requirements and functionalities

- Provisions of this Standard
- Regulatory and legal requirements
- Industry specific secure coding practices (OWASP)

d) Include in the agreement the right to audit clause

e) Conduct source code review to identify potential vulnerabilities, back-door and malicious code

f) Control the number, rotation and termination of staff involved in outsourced development activities to restrict:

- Unauthorized access
- Leakage of information

SA 6 Supply Chain Management

SA 6.1 Secure Acquisition [B] [S]

Prior to procurement, it is imperative for the entity to ensure that all highly critical third-party products and services conform to the information security requirements as well as comply with relevant laws, regulations, circulars, and standards. This is important to maintain a secure and compliant information environment.

The entity should:

a) Define an evaluation process for suppliers of information systems, system components, medical devices and services

b) Include federal and local government requirements as part of supplier review

The entity should obtain information security compliance and security assessment reports from third parties, as deemed necessary.

SA 6.2 Supply Chain Protection Strategy [A] [S]

The entity should develop a comprehensive information security strategy against supply chain threats to the information systems and application, medical devices and equipment
The entity should employ security controls to protect supply chain operations. Suppliers should maintain the confidentiality of the entity's assets, design specifications as well as details related to orders received from the entity. Such information may provide a third party the knowledge to compromise the entity. Supplier should be contractually bound to this requirement. In the bidding phase minimum information should be shared besides the actual scope of work.

The entity should:

a) Limit sharing of information, configuration and architecture with suppliers. When essential, share securely relevant and needed information through secure channel

b) Define system acceptance criteria for all new system purchase and ensure information systems, system components, and medical devices are genuine and are satisfying system acceptance requirements

c) Ensure a reliable (i.e., not modified to provide back-door access or covert channels) delivery of information systems, medical devices or system/devices components

d) Evaluate risks to its information systems, medical devices, services and support operations and employ security controls to protect supply chain operations

e) Agree with suppliers of systems, applications, medical devices equipment, etc.-related products/services on control measures and include them in the supplier contract

f) Prefer vendors that can provide multiple layers of support starting with local support. Where applicable perform vulnerability testing before putting the new system into production

g) Include in the contract:

- Right-to-Audit clause
- Non-disclosure requirements
- Terms to comply with entity information security policy and requirements
- Terms to comply with relevant federal and local government requirements

SA 6.3 Process to Address Weakness or deficiency [A] [S]

The entity should establish processes to address weakness or deficiencies in supply chain elements. Even with due diligence while contracting with suppliers, weaknesses may be found during the life of the contract. These may be found during audits, verification / validation or as part of vulnerability assessment or penetration testing. Regular assessments of suppliers are needed.

The entity should:

a) Identify and document supply chain elements and their interdependencies

b) Identify and address issues concerning supply chain elements

c) Conduct regular assessments and audits of supply chain elements

SA 6.4 Supply of Critical Information System Component [A]

The entity should ensure adequate supplies of critical information systems, medical devices and system/devices components. Unforeseen events or adversaries can impede organizational operations by disrupting the supply of critical information system components or corrupting supplier operations.

The entity should:

a) Engage with more than one supplier for critical products and systems

b) Establish contingency plans for the supply of any critical information systems, medical devices and system/devices components

c) Consider stockpiling of essential and critical spare components

d) Utilize multiple suppliers for critical components

Domain 10 - Information Security Incident Management

It is the entity management's responsibility to ensure the entity proactively prevents information security breaches and responds appropriately to incidents or near misses.

As the value of health information has grown exponentially worldwide it has become a soft target for malicious intent communities, individuals and nation states. They attempt to disrupt an entity's ability to conduct and sustain business or to be in business, and to disrupt the government's ability to provide healthcare services to its citizens and resident communities. Entity's utilization of technological advancement and innovation should not be limited to service delivery; rather it should also be to defend and respond to deliberate and accidental attempts to disrupt the entities' services.

An entity's ability to respond to and restore service after disruption attempts shows the entity management's commitment to its vision and objective values towards service delivery quickly and confidently. Entity management should be aware that information security incidents will not always be preventable. But adequate procedures, process and technologies to detect, report and handle incidents, combined with education and awareness, can minimize their frequency, severity and impact on an entity. This impact could be on healthcare delivery, assets, reputation, financial and legal.

It is essential that serious information security incidents that can potentially disrupt critical business processes and healthcare services are promptly communicated to the appropriate authorities so that they get involved early in the decision-making and communication. Contact information for the Abu Dhabi Health SOC , which is the 24/7 security operations center of the DoH is available in 5. Partnership of this document.

Objective:

To ensure that entities define and utilize suitable processes and resources to identify and respond to information security and privacy incidents, that they are not severely impacted by incident outcomes and that they are able to restore affected operations within an acceptable timeframe.

IM 1 Information Security Incident Policy

IM 1.1 Information Security Incident Management Policy [B]

The entity should develop, enforce and maintain an information security incident management policy, to manage and guide the entity's response to information security incidents

The policy should:

a) Be relevant and appropriate to the entity's operation and risk environment

b) Demonstrate management commitment, objectives and directions

c) Establish incident management roles and responsibilities

d) Establish a proactive, collaborative and sustainable process of identifying and resolving adverse information security incidents.

e) Establish management demands on:

- Incident identification
- Incident response
- Incident notification/communication
- Learning from incident

f) Be read and acknowledged by involved internal and external stakeholders

Depending on the size and structure of the entity, the Information Security Incident Management policy can be included as part of a single general information security policy document or can be split up into multiple policies that reflect the complex nature of the entity.

To facilitate entity policy development process, the DoH has provided sample Baseline Policies in Section 3 of this document. Entities are free to customize the provided baseline policies as per their environment as long as they remain compliant with the requirements of the ADHICS Standard and any other DoH or legal s.

Note that, besides the Information Security Incident Management Policy, this domain has the following supporting or dependent entity policy references:

1. Access Control Policy
2. Communications and Operations Management Policy
3. Third party security policy
4. Compliance Policy

IM 2 Incident Management and Improvements

IM 2.1 Incident Response Procedure [B] [S]

The entity should establish process(es) to guide information security and cyber security incident response activities

The entity management should acknowledge that not all threats can be prevented and, therefore, the speed to resolution upon detection is critical. Improving incident response processes and removing bottlenecks is the way to reduce impacts.

Information security incidents can include corruption or unintentional disclosure of critical health information or the loss of availability of healthcare information systems, where such a loss adversely affects healthcare delivery or results in adverse clinical events.

The process(es) should:

a) Have tested procedures to handle incident during preparation, detection, analysis, containment, eradication, and recovery

b) Clearly document roles and responsibilities of the relevant stakeholders and management

c) Establish a formal channel for entities and external stakeholders to report information and privacy events and weakness in any information asset as soon as they are identified

d) Assess information security events and/or alerts and determine if they are to be categorized as incident

e) Inform the Abu Dhabi Health SOC of information security and privacy incidents within predetermined timeframes

f) Escalate internally within the entity and externally to Abu Dhabi Health SOC, if the incident is not resolved timely

g) Ensure the incident notification includes all the information as requested by DoH. This includes

h) Connect incident handling activities with contingency planning activities

Information Security Incident Classification

Priority	Alert Level	Activity Description	Impact
P1	**Critical/Catastrophic (Very High Risk)**	Threat of, or actual, malicious cyber activity (hacking, viruses, or other activity) that will disrupt, destroy, or degrade services and infrastructure. Incident occurred, is imminent, or is ongoing. Zero-day exploit has been released and is expected to target entity's systems. The incident will seriously impact entity's Information and related assets or reputation and will require immediate action.	Potential or observed total or near-total destruction, degradation, or compromise of entity's Infrastructure and services. Potential or observed serious and widespread degradation or destruction, threatening continued operation of entity's critical services Known significant impact of zero-day exploit discovery or release exists Normal business operations and functions may be indefinitely suspended Major harm to the reputation of the government. Profound loss of confidence in the credibility, integrity or competency of government, by the citizenry and international partners.
P2	**Severe (High Risk)**	Threat of, or actual, increased malicious cyber activity (hacking, viruses, or other activity) directed at national critical service(s) exists. Known or expected targeted intrusion or exploit of an entity providing a national	Potential for or observed major degradation, disruption and/or destruction of entity's Infrastructure and services Potential for or observed high level of degradation, disruption, or

		critical service is present or reported Zero-day exploit has been released, The incident affects entity's Information and related assets and should be dealt with as soon as possible. Any incident involving Law enforcement agencies will have an automatic High Impact level.	damage Impact of zero-day exploit discovery or release is unknown.
P3	**Elevated** **(Medium Risk)**	Threat of, or actual, increased malicious cyber activity (hacking, viruses, or other activity) exists. Known (suspected exploiting known vulnerabilities and weaknesses) or expected intrusion or focused attack is present or reported. Zero-day exploit discovery or release is expected.	Limited or intermittent loss of confidence by citizens and other stakeholders in the design and execution of government services. Potential for or observed compromise and/or service is diminished in entity's Infrastructure and services Potential for or observed moderate level of degradation, disruption or damage with likelihood for more degradation, disruption, or damage. No significant impact has occurred from zero-day exploit.
P4	**Normal** **(Low Risk)**	Threat of, or actual, malicious cyber activity (known hacking, viruses or other malicious activity) presents only a general concern The Incident that does not affect any elements of the entity's Information and related assets but may initiate certain action and should be monitored in case of any change in the impact levels.	Non-critical systems are affected; critical services are not targeted or affected Potential impact is manageable by the responsible owner/operator

Information Security Incident Reporting Matrix

		Incident Notification to AD Health SOC	Incident Updates to AD Health SOC	Incident Resolution Communication to AD Health SOC
P1: Critical/ Catastrophic (Very High Risk)	**SLA**	Near-Real Time	Near-Real Time	Within 30 mins of incident resolution
	Mode of Communication	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone
	Responsible Stakeholder	Entity Point of Contact	Entity Point of Contact	Entity Point of Contact
P2: Severe (High Risk)	**SLA**	Within 1 hour of Incident acknowledgement	Every 1 hour	Within 1 hour of incident resolution
	Mode of Communication	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone
	Responsible Stakeholder	Entity Point of Contact	Entity Point of Contact	Entity Point of Contact
P3: Elevated (Medium Risk)	**SLA**	Within 1 hours of incident acknowledgement	Every 2 hours	Within 4 hours of incident resolution
	Mode of Communication	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone
	Responsible Stakeholder	Entity Point of Contact	Entity Point of Contact	Entity Point of Contact

P4: **Normal** **(Low Risk)**	**SLA**	Within 24 hours of incident acknowledgement	Every 24 hours	Within 8 hours of incident resolution
	Mode of Communication	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone	Primary: Email Secondary: Phone
	Responsible Stakeholder	Entity Point of Contact	Entity Point of Contact	Entity Point of Contact

Incident Acknowledgement: The average time it takes to acknowledge and prioritize a possible security incident

Incident Resolution: The average time it takes to fully resolve an incident. It shall be calculated from the time the incident gets acknowledged

Incident Notification to AD Health SOC: The average time in which the entity shall notify DoH- AD Health SOC about the incident. It shall be calculated from the time the incident gets acknowledged within the entity

Near Real Time (Incident Notification to AD Health SOC): Once the incident is acknowledged, the entity will promptly notify the Department of Health, ensuring minimal delay between incident acknowledgement and notification to DOH

Incident Updates to AD Health SOC: The average time in which entity shall provide updates to DoH about incident status and measures being taken. It shall be calculated after notifying DoH- AD Health SOC about the incident

In case the security incident involves breach of PII and PHI, the entity shall further adhere to the requirements of DP 1.7 “Data Breach Management”

IM 2.2 Computer Security Incident Response Team [A]

The entity should establish a Computer Security Incident Response Team (CSIRT) responsible for incident management and response efforts.

The CSRIT will have members from the management as well as various support departments like information security, IT, network team, facility security team etc.

Large Hospitals face an increasing amount of cyber security risks. Having a defined team raises awareness and readiness to respond to an incident.

The CSIRT should have specialized knowledge in intruder threats and attacks, as well as mitigation and resolution techniques. It shall establish an escalation procedure to quickly and effectively share pertinent information with customers and stakeholders.

The entity should:

a) Establish CSIRT with adequate authority, essential roles and responsibilities

b) Identify and nominate competent resources for each identified role of the CSIRT

c) Establish communication and response protocols

d) Allocate adequate funds for CSIRT operations

e) Ensure CSIRT coordinates with its counterparts and DoH for incidents which will have significant impact on the entity's assets or operations

f) Conduct information security forensic analysis, as required

g) Participate in forensics and the national incident response effort, as required

h) Identify impactful reoccurring incidents and implement controls to reduce the likelihood

i) Ensure lessons learnt from past information security incidents are maintained and shared with relevant stakeholders to aid in:

   - Addressing future information security incidents
   - Minimizing the recurrence of such incidents

j) Build knowledge database on information security incident diagnosis and response

k) Provide suitable training to members of the CSIRT to cover:

- Past incidents and lessons learnt
- Current threat environment of the entity
- New threats and attack trends across the world

IM 2.3 Incident Classification

The entity should assess and classify information security incidents.

A suggested Information Security Incidents Classification scheme is provided as a template for the Information Security Incidents Management Policy provided in Section A of this document. Classification of incidents will help prioritize the response.

The entity should:

a) Establish an incident classification scheme which captures the requirements of matrix recommended by DoH

b) Define workflows to handle incidents of various classifications/severity

IM 2.4 Incident Response Testing [T]

The entity should test its Computer Security incident response capabilities.

Incident response testing is a simulation of an actual incident. Based on identified information security incident scenarios, the testing will help identify the shortcomings of the procedures. In the absence of actual security incidents, regular simulations will keep the members aware of their roles and responsibilities.

The entity should:

a) Develop test procedures to validate the effectiveness of its incident response capabilities periodically

b) Establish the expected outcome of test and compare test results to identify gaps

c) Modify process and procedures to address gaps identified

d) Share tests results with the management

IM 2.5 Incident Records [T]

The entity should document and preserve records on all information security incidents.

Documenting information security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

The entity should:

a) Identify all relevant data and evidence to be collected during and after realization of an information security incident

b) Establish procedures for collecting evidence considering the:

- Chain of custody
- Safety of evidence
- Safety of personnel
- Roles and responsibilities of personnel involved
- Competency of the personnel
- Documentation
- Briefing
- Other identified requirements

c) Prepare a damage assessment report

d) Conduct a post incident analysis and implement controls identified as recommendations

e) Preserve documents, records, reports and evidences in compliance with the entity's retention policy

IM 3 Information Security Events and Weakness Reporting

IM 3.1 Situational Awareness [A]

The entity should develop a situational awareness culture by participating in the information sharing community and obtaining cybersecurity information from various sources.

Additionally, a comprehensive set of partnership initiatives are also being developed by the DoH to contain and limit exposure to information security threats across the healthcare sector. These include Awareness E-Learning, Security Advisories, Newsletters, Cyber Threat Intelligence (Brand & Digital Asset Monitoring), Forensic Assessment, Vulnerability & Technical Assessment, and a Threat Intelligence Platform providing actionable threat intelligence feeds to entities, specific to their deployed assets. This will leverage the investments, resources and technologies of DoH to reduce the risk exposure across the Abu Dhabi Healthcare sector. These initiatives have been branded as the Abu Dhabi Health SOC

The entity should:

a) Identify priority information and share it internally to build the entity's business model based-context

b) Ensure all identified cybersecurity information is relevant to the:

- Entity's business operations
- Entity's information system and application, medical devices and equipment
- Entity's processes and control environment
- Entity's risk environment

c) Establish and coordinate with the healthcare sector regulator of Abu Dhabi to receive relevant cybersecurity information

Domain 11 - Information Systems Continuity Management

Information systems and applications have become fundamental to a modern medical facility's operations. The ability of an entity's systems and applications to support identified critical services and processes in adverse conditions is a measure of the maturity of the entity's operational capabilities.

Entities shall have proactive strategies and plans in place to counteract interruptions to entity operations and to protect critical business processes from the consequences of significant information system failures to enable timely resumption of affected processes

Due to high availability requirement of healthcare to the general public, a major effort should be put into resilience and redundancy arrangements, not just for the technology parts, but also for the cross-training of health personnel.

The objectives of this domain's controls are

To ensure systems, applications and resources are available to support service continuity requirements of identified critical services and processes during adverse situations or environment.

SC 1 Information Systems Continuity Management Policy

SC 1.1 Information Systems Continuity Management Policy [A]

The entity should develop, enforce and maintain an Information Systems Continuity Management policy to manage scenarios that challenge the continued availability of information systems and applications supporting critical business services.
The policy should:

a) Be relevant and appropriate to the entity's information systems and applications continuity demands. Consider the impact and likelihood of the risks faced. Any impact on a healthcare entity will also impact the public depending on their affected services

b) Demonstrate management commitment, objectives and directions. This policy will guide the development of the plans. Management commitment is required for financial, organizational, technical, and environmental resources to address the identified information security continuity requirements

c) Establish roles and responsibilities of involved stakeholders. More than one person should be required for each. Consider cross-training staff for redundancy.

d) Establish management expectations on:

- Planning for information system and application continuity during adverse situations
- Ensuring Information security during business continuity and disaster recovery
- Compliance with organizational business continuity plans
- Testing of continuity and restoration plans

Depending on the size and structure of the entity, the Information Systems Continuity Management policy can be included as part of a single general information security policy document or can be split up into multiple policies that reflect the complex nature of the entity.

To facilitate entity policy development process, the DoH has provided sample Baseline Policies in Section 3 of this document. Entities are free to customize the provided baseline policies as per their environment as long as they remain compliant with the requirements of the ADHICS Standard and any other DoH or legal requirements.

Note that, besides the Information Systems Continuity Management Policy, this domain has the following supporting or dependent entity policy references:

1. Incident Management Policy
2. Information Systems Continuity Policy
3. Information Systems Continuity and Recovery Plan
4. Communications and Operations Management Policy
5. Compliance Policy
6. Backup Policy

SC 2 Information Systems Continuity Planning

SC 2.1 Business Impact Analysis [A] [S]

To maintain operational resilience and continuity of operations during and after a business disruption, a business impact analysis (BIA) is the process of assessing the criticality of business activities and the accompanying resource requirements. The BIA calculates recovery time objectives (RTOs) and recovery point objectives (RPOs) as well as the effects of disruptions on service delivery and hazards to service delivery. The development of strategies, solutions, and plans is then guided by these recovery criteria.

The BIA shall be carried out annually or when changes take place in the environment.

The entity should:

1. Perform Risk Assessment to identify points of failure and understand likelihood, impact in time for identification and prioritization of critical business systems and applications
2. Determine the criticality of entity information systems and their need for recovery
3. Establish Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to resume activities timely and effectively
4. Identify dependencies between services and supporting resources (facilities, personnel, equipment, software, data files, system components, and vital records)

SC 2.2 Developing Information Systems Continuity Plans [A] [S]

The entity should develop Information System Continuity Plans that shall prevent or minimize interruptions and support in recovery of critical business services and processes during adverse situations.

The information systems and application continuity plans should align with the entity's business continuity plans.

The entity shall identify its critical business information systems and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport, and facilities. If the planning entails moving to an alternate site, this new site should also meet the information security requirements met by the primary

site.

The plan should:

a) Enlist information systems in scope of continuity plan

b) Identify continuity requirements for recovering from events that affect availability of critical system and applications

c) Have recovery strategies for critical systems and applications to minimize the period and impact of disruption

d) Be harmonized and support organizational business continuity planning and/or disaster recovery demands

e) Identify individuals with assigned roles and responsibilities, along with necessary contact information

f) Define call tree matrix and escalation matrix

g) Defined criteria and conditions for plan activation

h) Have provisions to address information security incident-based scenarios and provide guidance to operate and support critical business services during such scenarios

i) Ensure required level of continuity for information security during disruption

j) Consider redundant system, components or architectures for critical business services, processes and technology, wherever availability cannot be guaranteed using the existing systems architecture

SC 2.3 Testing, Maintaining and Reassessing Plans [A]

The entity should test, reassess and maintain its information systems continuity plans at planned intervals a minimum annually or in case of any significant change, to ensure that they are up to date and effective.

An information systems and application continuity plan is in place to respond to threats to data security, including significant data breaches, and it should be tested once a year as a minimum, with a report to senior management.

Health facilities also need to ensure that the plans that they develop are regularly tested in different ways like using checklists, tabletop simulations, modular testing and full rehearsals.

The entity should:

a) Define schedules and test information system and application continuity plans to ensure:
    - Adequacy and effectiveness of the plan.
    - The entity and resource readiness to execute the plans
b) Conduct fail over testing to check the efficiency of redundant information systems
c) Document test outcomes and lessons learned
d) Assess plan adequacy during changes to business services, systems and applications
e) Update and maintain information system and application continuity plans based on lessons learned and assessment outcome

Section 5

Useful Forms & Templates

This section contains the list of forms which are specific to the procedures defined for certain policies.

Forms

1. Awareness and Training Calendar
2. Awareness and Training Attendance
3. Information Security Violation Management Process
4. New User creation
5. Access Review Record
6. Visitor Log Register
7. Asset Inventory
8. Asset Disposal Form
9. Legal and Compliance Register
10. Backup Request Form
11. Change Request Form
12. Key Log Register
13. Third party security assessment
14. Information Security Incident Reporting Form
15. Consent Collection
16. Data Privacy Impact Assessment
17. Data Breach Notification
18. Exit Clearance Form

Section 6

Continual Improvement

This section describes the activities required post implementation of the controls for continually improving the effectiveness as part of the PDCA cycle.

Continual Improvement

Internal Audit

The internal audit is a process of checking the compliance with the requirements of ADHICS, and the information security policies in the entity. This is a periodic activity performed by qualified auditors who have clear understanding of the ADHICS controls and the information security processes of the entity. The main objectives of internal audit are to:

1. Identify non-conformities with requirements of ADHICS;
2. Verify conformance to the relevant legislation or regulations requirements;
3. Verify conformance to the identified information security requirements in the entity;
4. Verify that the applicable ADHICS controls have been implemented and maintained effectively;
5. Verify that the control measures perform as expected, according to the predefined Key Performance Indicators (KPIs)

Corrective and Preventive Action

This Corrective Action and Preventive Action (CAPA) procedure is to ensure the continual improvement of the Information Security Management Systems (ISMS) and maintaining the objectives in place in the entity through the use of audit results, analysis of monitored events, corrective and preventive actions and management review. This continual improvement includes:

1. Corrective actions to eliminate the cause of non-conformity with the control requirements in order to prevent recurrence;
2. Preventive action to eliminate the cause of potential non-conformities in order to prevent their occurrence.

Management Review

The purpose of the MR procedure is to define the process for management commitment and review of the currently implemented Information Security Management System:

1. Ensure that management reviews the ISMS;
2. Specify the continuous suitability, adequacy and effectiveness of the ISMS;
3. Identify major risks for non-compliance;

4. Assess opportunities for improvement;
5. Identify the need for changes to the ISMS, including information security policy and information security objectives;
6. Prove adequate documentation/records.

The Management Review of the ISMS should occur at the IS Committee not less than once per year. The IS Manager will take overall responsibility for follow-up activities approved during the previous Management Review meeting. Progress and developments on actions resulting from the Management Review will be documented as part of the ISMS Committee meeting minutes. Follow-up action will not be considered complete until all corrective actions or measures have been implemented and recorded in the ISMS Committee meeting minutes as being complete.

Effectiveness Measurement [KPI]

Measuring the effectiveness of selected controls is an essential prerequisite for continuous improvement of the ISMS and requirements of the ADHICS standards. The purpose of this procedure is to apply various measurements within the scope of the ISMS in the entity and to analyze and use this information for more effective and efficient management of information security.

Measurements should be based on well-defined metrics, which serve as a basis for making decisions concerning information security management processes and controls. These measurements may be used in an assessment of how well the security objectives are met.

Sample metrics given below:

Metric	Findings raised by External and internal ISMS audits & Technical assessments
Description	Measurement of the effective implementation of the Continual Improvement Procedure
Scope of the metric	ISMS Scope
Objectives	To ensure that corrective and preventive actions are effective and timely implemented
Measured by	Information Security Manager
Method	Analysis, counting, normalize
Source	External and Internal audit reports, technical assessment reports & follow up documentation

Procedure	The Information Security Manager will review the reports and follow up documentation. The findings will be counted (Value A). Findings where the resolution/resolution plan is overdue for more than one month will be counted (B). I = B divided by A multiplied by 100. Integer value only.
Frequency	Yearly
Date	February every year
Indicators	I < 10% good, no action required 20% ≤ I ≤ 30% acceptable, investigate reason for not meeting the target. I > 30 % not acceptable, corrective actions

Section 7

Compliance Monitoring & Reporting

This section describes the requirements for monitoring the compliance levels of entities and reporting the same to the DoH

Compliance Monitoring & Reporting

Compliance

Implementation of the applicable Information Security control criteria should be monitored periodically to ensure they are adequate, appropriately implemented, maintained and that associated responsibilities, deliverables, and timelines are documented and reported.

Self-assessment checklists will be used for ADHICS compliance monitoring. This checklist includes all 131 controls and their sub-controls. Entities need to provide documentary evidence for any control they classify as 'Not Applicable' to them. An external audit on compliance to the ADHICS standard is integrated into the existing health facility audit program and linked with facility licensing (new facility registration & renewals).

Similarly, mandatory e-Learning on information security provided by DoH will be added to the existing CME program as part of health professional licensing Detailed information on these compliance initiatives will be published as they are implemented.

The specific requirements for Malaffi onboarding are not part of the scope of this document. The ADHICS standard sets the overall security baselines for Health Information protection. It is a government mandate that Health Information be considered as highly classified data element, to be protected through its lifecycle. Entities should establish control measures that will prevent and minimize probabilities of:

1. Unauthorized access and/or usage of healthcare data
2. Unauthorized or accidental modification of healthcare data
3. Leakage of healthcare data
4. Loss of healthcare data

Reporting

The entities should review and submit their updated compliance status to DoH, as part of periodic compliance reporting, highlighting road map timelines and deviations.

Section 8

Baseline Checklists

This section consists of selected check lists which will be helpful in the verification of the compliance requirements for different domains or functions.

Baseline Checklists

General Checklist

☐ Information Security Governance committee established.

☐ Information Security roles defined.

☐ Information Security roles assigned.

☐ Registered domain for web and email.

☐ Information Security policy developed and published.

☐ All Policies are read and acknowledged by users.

☐ Information security scope defined.

☐ All Information Assets are inventoried and accounted for.

Password Checklist

☐ Policies are in place prescribing password practices for the [Entity Name.

☐ All staff understand and agree to abide by password policies.

☐ Each staff member has a unique username and password.

☐ Passwords are not revealed or shared with others.

☐ Passwords are not written down or displayed on screen.

☐ Passwords are hard to guess, but easy to remember.

☐ Passwords are changed routinely.

☐ Passwords are not re-used.

☐ Any default passwords that come with a product are changed during product installation.

☐ Any devices or programs that allow optional password protection have password protection turned on and in use.

Anti-Virus Checklist

☐ Policies are in place requiring use of anti-virus software.

☐ All staff understand and agree that they shall not hinder the operation of anti-virus software.

☐ All staff know how to recognize possible symptoms of viruses or malware on their computers.

☐ All staff know what to do to avoid virus/malware infections.

☐ Anti-virus software is installed and operating effectively on each computer in compliance with manufacturer recommendations.

☐ Anti-virus software is set up to allow automatic updates from the manufacturer.

☐ Anti-virus software is fully up to date according to manufacturer's standards.

☐ Handheld or mobile devices that support anti-virus software have it installed and operating.

Access Control Checklist

☐ Policies are in place prescribing access controls.

☐ Every user account can be positively tied to a currently authorized individual.

☐ Users are only authorized to access information which they need to know to perform their duties.

☐ All files have been set to restrict access only to authorized individuals.

☐ All staff understand and agree to abide by access control policies.

☐ Computers running healthcare-related systems are not available for other purposes.

Physical Access Checklist

☐ Policies are in place prescribing the physical safety and security of devices and devices.

☐ All staff understand and agree to abide by physical access policies and procedures.

☐ Computers are protected from environmental hazards.

☐ Secure Areas are identified with designated owners.

☐ Physical access to secure areas is limited to authorized individuals.

☐ Computers running EMR systems are shielded from unauthorized viewing.

☐ Equipment located in high-traffic or less secure areas is physically secured.

☐ CCTV are installed in all identified secure areas.

☐ Visitor logs are recorded for all identified secure areas.

☐ Cabinets are locked with access of keys limited to authorized individuals.

☐ Private areas to discuss Protected Health Information (PII and PHI).

☐ Utilities; HVAC systems, Fire suppression, Emergency power generators are installed, as required.

Network Access Checklist

☐ Policies are in place prescribing network configuration and access.

☐ All staff understand and agree to abide by network use policy.

☐ Access to the network is restricted to authorized users and devices.

☐ Guest devices are prohibited from accessing networks containing PII and PHI

☐ Wireless networks use appropriate encryption.

☐ Computers contain no peer-to-peer applications.

☐ Public instant messaging services are not used.

☐ Private instant messaging services, where used, are secured appropriately.

Backup and Recovery Checklist

☐ Policies are in place prescribing backup and recovery procedures.

☐ All staff understand the recovery plan and their duties during recovery.

☐ Files identified as critical are documented and listed in the backup configuration.

☐ Backup schedule is timely and regular.

☐ Periodic restoration tests are performed, and evidence retained.

☐ Backup media are physically secured.

☐ Backup media stored offsite are encrypted.

☐ Backup media are made unreadable before disposal.

Maintenance Checklist

☐ Policies are in place prescribing EMR system maintenance procedures.

☐ Staff with responsibilities for maintenance understand and agree to system maintenance policies and procedures.

☐ Computers are free of unnecessary software and data files.

☐ Vendor remote maintenance connections are documented and fully secured.

☐ Systems and applications are updated or patched regularly as recommended by the manufacturer.

☐ Evidence are available for Periodic maintenance of Physical and environmental supporting utilities such as CCTV, AC, DG, Fire protecting equipment.

Mobile Devices Checklist

☐ Policies are in place prescribing use of mobile devices.

☐ All staff understand and agree to abide by mobile device policy and procedures.

☐ Mobile devices are configured to prevent unauthorized use.

☐ PII and PHI on mobile devices is encrypted.

☐ Connections between authorized mobile devices and EMRs are encrypted.

Firewall Checklist

☐ Policies are in place prescribing the use, configuration, and operation of firewalls and firewall logs.

☐ All networks are protected by a properly configured firewall from external networks.

☐ All staff understand and agree that they may not hinder the operation of firewalls

☐ Appropriate content filtering is implemented such as blocking of malicious web sites.

☐ Remote access is restricted

4.Relevant References Documents

No.	Reference Date	Reference Name	Relation Explanation / Coding / Publication Links
1	2019	Abu Dhabi Healthcare Information and Cyber Security Standard	AAMEN | Department of Health Abu Dhabi (doh.gov.ae)
2	2019	Federal Law No. (2) of 2019 on the Use of Information and Communications Technology (ICT) in healthcare	https://mohap.gov.ae/app_content/legislations/php-law-en-77/mobile/index.html#p=1
3	2021	Federal Decree-Law no. (45) of 2021 On Data Privacy	https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws
4	2023	GP Program_National IoT Security Policy	Policies (csc.gov.ae)
5	2023	GP Program_National Cloud Security Policy	Policies (csc.gov.ae)
6	2020	Department of Health Publications: Data Privacy & Internet Of Medical Things Standard, Circulars	AAMEN | Department of Health Abu Dhabi (doh.gov.ae)
7	2020	UAE Information Assurance Regulation	https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation
8	2017	Abu Dhabi	https://data.abudhabi/opendata/sites/default/f

		Government Data Management Standards V2.0	iles/AD-Gov-Data-Management-Standards-EN-v1.0.pdf
9	DRAFT	DOH Standard on Telemedicine	Yet to be released
10	2022	ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html
11	2015	ISO/IEC 27017:2015	https://www.iso.org/standard/43757.html
12	2023	HITRUST	HITRUST Alliance | HITRUST CSF | Information Risk Management
13	2009	Information Security Governance – A Practical Development and Implementation Approach, by Krag Brotby	[PDF] Information Security Governance by Krag Brotby eBook | Perlego
14	2021	NCEMA	Publication-en.pdf.aspx (ncema.gov.ae)
15	2019	ISO22301:2019	ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements
16	2016	ISO 27799:2016	ISO 27799:2016 - Health informatics — Information security management in health using ISO/IEC 27002

5.Revision List (Changes)

Issue No.	Revision Date	Clause No.	Revision Explanation (changes)
V2.0	Jan 2023	Whole Document	Updated based on healthcare industry trends, technology advancements, regional laws, regulations, standards, and international best practices
V1.0	Feb 2019	Initial Release	Initial Release