دائـــــرة الـــصـــحـــة
DEPARTMENT OF HEALTH

GUIDELINES FOR THE IMPLEMENTATION OF THE ABU DHABI HEALTHCARE INFORMATION AND CYBER SECURITY STANDARD

[ADHICS]

December 2019

PUBLIC عـــام

This document does not contradict with any other document issued by the Department of Health. In case of contradiction, please refer to the documents concerned and follow them. This Document is "Guidelines" and is only to manage Information Security.

Introduction

The Department of Health (DOH) has established the Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard as a strategic initiative in support of DOH's vision and Federal/National mandates, endorsed by DOH's Executive Committee. The provisions of this Standard are harmonized with international healthcare industry standards for Information Security.

The adoption of ADHICS Standard by DOH licensed healthcare entities will prepare and enable Abu Dhabi's Health Sector to uphold privacy and security. Its implementation complements the Government's initiatives towards Health Information Exchange (HIE), enhancing security and public trust.

Legal Background

The Federal Law No. (2) for the year 2019 on the use of Information and Communications Technology (ICT) in Healthcare mandates security and safety of health information while also specifying hefty penalties for non-conformance. Implementing the ADHICS standard will significantly improve the entity information security risk profile but does not exclude the entity from any legal liabilities.

Also, the Telecommunications Regulatory Authority (TRA) National Cybersecurity Strategy has identified the Healthcare Sector as one of the nine critical sectors of the UAE. The National Cybersecurity Strategy envisages identifying critical assets, establishing risk management standards and a robust process for reporting, compliance and incident response. The DOH Cybersecurity strategy complements the National Cybersecurity Strategy, adapting it to the Abu Dhabi Healthcare sector.

Purpose of this document

This document aims to provide a common set of guidelines to help DOH-licensed healthcare entities in the development, implementation, establishment and maintenance of Information Security Management System (ISMS) Program required for the health and other information under their control.

There is widespread awareness about Cybersecurity incidents due to coverage in news media. However, awareness about the root causes as well as the full implications of these incidents is low. It is only a matter of time before every entity faces an information security threat. How to minimize the impact and minimize the recovery times is critical for healthcare entities to maintain their service levels as well as legal and regulatory commitments.

As healthcare information becomes digitalized and healthcare equipment more and more 'connected', the risks are exponentially rising.

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.

There are new and disruptive digital innovations in the healthcare industry on a regular basis. 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. Having information security as a criterion in all phases like selection, procurement, contract, implementation and maintenance will minimize the risk and the need for workarounds later.

This guideline interprets "how" the elements mentioned in the ADHICS Standard can be implemented. Therefore, its focus is primarily 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. Entities that have already implemented other standards, such as ISO 27001, are already compliant with a majority of the ADHICS control requirements. However, particular attention will have to be paid to healthcare specific variations mandated by ADHICS.

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

The content of the standard and this guideline, while comprehensive, is not exhaustive. It is the healthcare entities' management responsibility to provide and maintain healthcare information security. Compliance to the ADHICS standard without due consideration of the actual business environment may not protect the information's confidentiality, integrity and availability.

Scope

The guidelines are 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 the DOH licensed healthcare entities, as well as the entities' access and usage of partners' and third party systems, and Information Technology applications utilized within Abu Dhabi Healthcare ecosystem. This includes the Shafafiya portal, Malaffi, the Health Information Exchange platform, DoH e-Services, Medical Tourism portal, etc. With respect to health information, the ADHICS standard is applicable to all forms of information, physical or digital. Please see Section A-2.1 of the standard for details.

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-6 of the standard explains the applicability of the controls depending on the three categories of entity.

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 a healthcare entity's capability to secure its information assets, continue functioning and delivering its healthcare activities without interruption. At the same time, the Department of Health is building and enhancing its cybersecurity capabilities to complement the efforts of Abu Dhabi healthcare entities. These efforts include a 24/7 Security Operations Center (SOC) to support cyber incident management across the Abu Dhabi healthcare sector in addition to its core information security activities for the DOH.

Additionally, a comprehensive set of partnership initiatives are also being developed by the Department of Health 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 the Department of Health to reduce the risk exposure across the Abu Dhabi Healthcare sector. These initiatives have been branded as the Abu Dhabi Healthcare CERT.

More Information:

For more information on or support from Abu Dhabi Healthcare CERT, please contact (24/7):
soc@doh.gov.ae
+971 2 4193 777

For more information and support on the Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard, please contact:
ADHICS@doh.gov.ae

Section 1

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

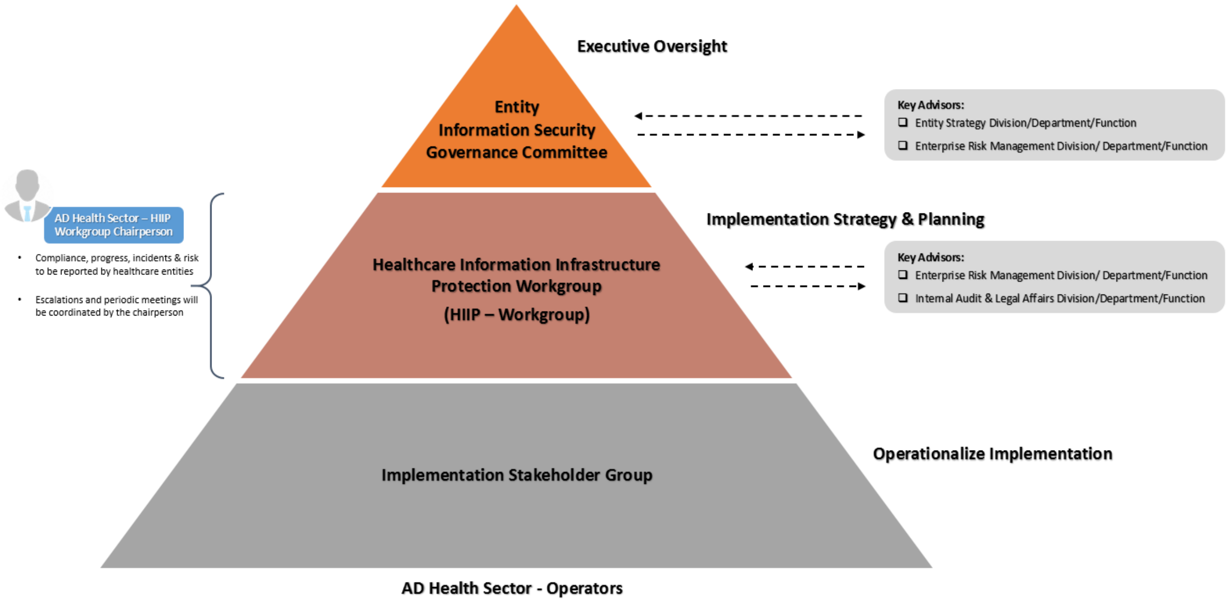
Step 1	**Obtain a copy of the standard**	**The standard is available for free download from Department of Health website** **(doh.gov.ae > Resources > Standards)**
Step 2	**Know your Entity license type**	Pharmacy, Clinic, Centre, Hospital etc.
Step 3	**Identify the control applicability**	Basic, Transitional or Advanced (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.

Governance

All DOH regulated healthcare entities must implement the three-layer ADHICS Governance pyramid structure specified in Section A-3 of the Standard.


Executive Oversight
Entity
Information Security
Governance Committee
Key Advisors:
❑ Entity Strategy Division/Department/Function
❑ Enterprise Risk Management Division/ Department/Function
AD Health Sector – HIIP Workgroup Chairperson
• Compliance, progress, incidents & risk to be reported by healthcare entities
• Escalations and periodic meetings will be coordinated by the chairperson
Implementation Strategy & Planning
Healthcare Information Infrastructure
Protection Workgroup
(HIIP – Workgroup)
Key Advisors:
❑ Enterprise Risk Management Division/ Department/Function
❑ Internal Audit & Legal Affairs Division/Department/Function
Operationalize Implementation
Implementation Stakeholder Group
AD Health Sector - Operators

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. 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 for audit purposes.

The HIIP Workgroup will be the interface between the entity and the Abu Dhabi Health Sector HIIP Workgroup 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.

Risk Management

Risk Management including assessment and mitigation requirements of ADHICS are covered in Section A-4 of the Standard. An entity's risk assessment process should treat health information security as a major risk taking into account health information privacy as well as availability of health information. Entities without an existing risk register can use an up to date asset register and the controls of Section B of the ADHICS standard to develop the entity risk register.

Risk assessment can guide a healthcare entity in determining the level of effort and resources needed to protect confidentiality, integrity and availability. The results of regular risk assessment must be aligned with the implementing entity's priorities, initiatives and investments..

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

Asset Classification

Section A-5 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 processing, storing, communicating and sharing. The following are considered information assets:

- Information (in physical and digital forms)
- Medical device and equipment
- Applications and Software
- Information System

- Physical Infrastructure (Data centre, access barriers, electrical facilities, HVAC systems, etc)
- Human resources (in support of 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 a healthcare entity. They can be used by the healthcare entity as is by just replacing the square brackets [ ] with the correct names as applicable to the specific entity. Alternatively, the healthcare entity can customize them to suit its purposes taking into account inclusion of all required information. Or, the healthcare entity may use its own policies if already in place. The term 'Users' means all employees, third parties and vendors who access the entity information in any form.

Index

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 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 compliance to this policy within their area(s) of concern.
6. The [***Director General or job title assigned with responsibilities of Entity's higher management***] of [***Entity Name***] shall endorse this policy for its effective implementation.

Policy in Detail

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 & 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. Where appropriate these principles are elaborated below to provide the basis by which [***Entity Name***] security will shape the direction and conduct of security:

1. Maintain the confidentiality, integrity & availability of Information & Information assets.
2. Meet the UAE regulatory, statutory and legislative requirements.
3. Report and investigate all suspected breaches of Information Security.
4. Provide appropriate Information Security Training & awareness to all employees (permanent & contract employees).
5. Design appropriate controls and procedures to support the implementation of this Information Security Policy.
6. Ensure all stakeholders are responsible for implementation of respective security policies & procedures within their area of operation, and oversee adherence by their team members.
7. Continually improve Information Security through implementation of corrective and preventive actions.
8. Prepare, maintain and test Business Continuity Plans in a practical manner based on the business needs.
9. Annually review this Policy for adequacy and appropriateness.

Policy Compliance

1. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

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 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 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 implement the defined security controls and ensure compliance with this policy.

Policy in Detail

Note: Human resources management shall be in compliance with [***Relevant HR Law***] and its amendments, or any other regulations the Entity follows in this context.

Screening

1. 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:
    - Verification of personal data such as date of birth.
    - Verification of relevant educational and professional qualifications.
    - Verification of previous employment data.
    - An assessment of background, by seeking criminal records verifications through the official sources.

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):
    - Performance of daily activities in compliance with the Information security and all other relevant policies, procedures and standards.
    - 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 the information security policies of [*Entity* ***Name***].

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 awareness programs are conducted for new employees as part of an induction program.
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.
3. The [***Information Security Section/Department or the function assigned with information security responsibilities***] shall develop an annual Information Security Awareness and training plan. The awareness plan may cover:
    - Periodic emails on information security.
    - Conducting quiz and survey.
    - E-Learning modules covering information security best practices, etc.
    - Publishing Posters & flyers.
4. The [***Information Security Section/Department or the function assigned with information security responsibilities***] shall formulate the evaluation methods and criteria for measuring the effectiveness of information security awareness.

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. All employees who indulge in misconduct or a security breach shall be subjected to the HR disciplinary process after verification and collection of evidence.
3. Any serious misconduct or significant violation of Information security policies shall be referred to the Entity Disciplinary Committee for further action.
4. The formal disciplinary actions shall be decided considering the following factors:
    - Nature and gravity of the breach
    - Its impact on business
    - Whether it's a first or repeat offence
    - Whether the violator was properly made aware and trained
    - Relevant legislation
    - 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 Physical Access to [***Entity Name***] facilities 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.

Policy Compliance

1. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

Information Assets Management Policy

Objectives

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 healthcare entities to monitor and record the use of information assets.

Information assets includes information/data 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
- Applications and Software
- Information System
- Physical Infrastructure (Data centre, access barrios, electrical facilities, HVAC systems, etc.)
- Human resources (in support of care delivery)

Scope

This policy applies to all Users of [***Entity Name***]. The scope includes all information assets owned and managed by [***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 compliance to this policy within their area(s) of concern.
6. All information assets owners are responsible for ensuring that this policy is applied within their area of their responsibility.

Policy in Detail

Information Assets Management

1. All information assets shall be identified, recorded and maintained through an information asset inventory.
2. The asset inventory shall be reviewed and updated on regular basis and as and when there is any major organizational restructure.
3. All information assets shall have the following defined & documented:
    - Owner/Author of information.
    - Custodian of information.
    - Distribution list/Access control list.

Information Assets Classification Guidelines

1. The owners of the information assets shall be responsible for assigning/maintaining appropriate classifications based on the following criteria:
    - Value of content/information it holds or carries.
    - Intended Users of the information.
    - 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. The classification is wholly based on the examination of the value of the information, who will have access to the information assets, and the resulted 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 country. Information disclosure could potentially threaten life or seriously prejudice public order.	The compromise of information in this category could result in serious damage [***Entity Name***] financial status, of reputation of, customers trust, critical systems operations of legal implication etc..,	VIP health information, Critical health information, Credit Card Details, IP addresses, Network and Infrastructure Diagrams, etc.
Confidential	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,	The compromise of information in this category could result in damage to [***Entity Name***] competitive	Strategic/Critical Projects Contracts, payroll data, employee private records (medical records), audit reports, risks registers, assets

C0 M80 Y95 K0 R232 G78 B27 # E84E1B ORANGE	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/healthcare information, government information, financial information etc.).	advantage, strategic operational plans, government relations, legal binding.	registers, financial details in relation to projects or proposals, strategic/critical projects RFPs, 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/health sector. 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.

1. 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.
2. Any information where the classification is not obviously clear or not done shall be treated as Confidential **irrespective** of the content or the data it carries.

Information Assets Labeling

1. All information regardless of its form (electronic or physical) shall be classified and shall be appropriately labeled based upon the classification category identified.
2. All Information Systems or electronic data or information of [***Entity Name***] which are used for processing information, where physical labeling is not possible, shall be considered as Confidential**.**

Asset Labeling
Public C100 M0 Y100 K0 R0 G150 B64 # 009640 GREEN
Restricted C100 M0 Y0 K0 R0 G158 B227 # 009EE3 BLUE
Confidential C0 M80 Y95 K0 R232 G78 B27 # E84E1B ORANGE
Secret C0 M100 Y100 K0 R227 G5 B19 # E30513 RED

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.
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 stored according to the assigned classification category of information.

2. 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.
3. The recipient of the information shall treat it in accordance with the information asset classification established by its originator.
4. The information asset owner shall consider proper transmission controls for the information assets transmission requirements.

Information Assets Disposal

1. 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.
2. The information asset owner shall ensure that appropriate security controls are considered while disposing the information assets so that the information contained in it is irrecoverable. Suggested retention and disposal procedure is provided in the policy appendix – Information assets management procedure.

Policy Compliance

1. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

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;

- Physical protection of data center and information processing equipment(s)/facilities
- Physical entry control for secure areas
- Medical devices/equipment(s) protection
- Heating, ventilation, and air conditioning of critical areas and work places
- Supporting mechanical and electrical equipment's
- Surveillance of critical areas and work places
- Security and protection of physical archives
- Fire and environmental protection
- Visitor management

Scope

This policy applies to all Users of [***Entity Name***], and covers all types of information and information processing facilities 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 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 in Detail

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:
   - End of employee's service
   - Vendors/Contractors completing their engagement or as per the expiration of the temporary gate pass.
   - If requested by the Director of the department which the user belongs to.
   - 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***].

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. Visitors shall be escorted at all times by authorized employee while in [***Entity Name***] premises.
4. Users shall refrain from entering critical areas without getting proper approval from authorized employee.

5. All areas that contain critical information and information processing facilities shall be fitted with strong physical access control mechanisms.
6. Physical access shall be deactivated or revoked for terminated Users.
7. 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.
8. 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.
9. Users shall keep their cabinets/drawers locked when leaving the offices at the end of the day.

Secure Working Areas

1. 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.
2. 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.
3. Users shall refrain from smoking inside the premises of [***Entity Name***] apart from the designated smoking zones.
4. 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
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 emergency 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 section manager.

2. Information assets that are sent out for maintenance or repair shall be recorded by the respective section manager.
3. Retirement of information assets shall be authorized by the respective section manager and approved by the [***Corporate support Department 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.

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***].

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 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.

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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

Access Control Policy

Objectives

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

Scope

This policy applies to all Users of [***Entity Name***] who use or require Logical Access to information processing facilities as part of their day to day activities.

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 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 in Detail

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. User access provisioning should be initiated in the following cases, but not limited to:
   - New employment
   - Users being promoted/demoted/transferred

- Temporary assignment of job responsibilities
- Access to external Users (such as vendors, contractors and partners) & third parties, etc.

4. 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***].
5. Any information systems' service account or generic account shall be created with approval from the Information System Owner, Business Processes Owner & shall have an owner assigned to ensure accountability.
6. The list of service accounts or generic accounts shall be identified & documented by respective systems administrators.

User Access De-Provisioning

1. User Access de-provisioning is valid under the following circumstances:
    - End of User's service.
    - If requested by the Director/Manager of the concerned department
    - External Users such as (vendors, contractors and partners) & third parties, etc., completing their engagement.
    - If a User is found to have violated any policy or misused the provided access in any mean.
2. 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.
3. The [***HR section/department or the function assigned with HR responsibilities***] shall be responsible of defining procedure for access revocation due to resignation or termination of employees.
4. 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***].
5. 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.
6. 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 evidences.

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 on a regular basis, at least twice a year. 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.
2. 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.
3. All privileged and administrators accounts shall be reviewed on a quarterly basis, and changes to such accounts shall be logged for periodic review.

Network Security

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. Network and security devices placed on all external network connections, shall display banner message warning unauthorized Users that unauthorized use is prohibited (e.g. If you are NOT authorized to access this equipment, Please log out immediately).
9. All network and security devices shall be protected against physical and environmental threats in accordance with the Entity physical and environmental security policy.
10. 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.
11. Segregation, in the form of multiple DMZ's, shall be implemented when publishing public facing services.
12. Change management procedure and proper authorization shall be followed prior to modifying configurations of any network and security device.
13. [***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.
14. 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.

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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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 ID's at regular intervals.

Operations Security Policy

Objectives

To ensure that activities concerning support and maintenance of data, technology, and application are controlled and carried out in a standardized manner to reduce probabilities of errors and compromises, and to increase efficiency and security. Objective outcome of effective operations management includes, but is not limited to:

- Improved security and reduce probabilities of compromise
- Reduced errors
- Controlled unauthorized activities
- Regulated efforts
- Increased efficiency
- Reduced security incidents

Scope

This policy applies to all Users who are responsible of operating and managing [***Entity Name***]'s IT infrastructure and services.

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 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. [***IT section/department or the function assigned with responsibilities of IT Management***] is responsible to ensure compliance with this policy.

Policy in detail

Assets Inventory

1. All sections of [***IT section/department or the function assigned with responsibilities of IT Management***] shall ensure having an up to date inventory of information systems such as, software, servers, appliances, devices, tools, tokens, communication links, which are in use in [***Entity Name***]. The inventory shall also highlight the information systems that were de-commissioned.
2. Access to the information systems inventory shall be restricted within group of employees of [***IT section/department or the function assigned with responsibilities of IT Management***] and shall be shared strictly on a need to know basis.
3. All IT assets must be assigned with owner/custodian who must maintain perpetual inventory control, a record of the new location and new equipment custodian of all equipment issued to others.

Capacity Management

1. All sections of [***IT 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.
2. All sections of [***IT 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.
3. All sections of [***IT 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.

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).

Antivirus Management

1. All sections of [***IT 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.

Backup Management

1. Backup requirements shall be identified for all information systems 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 Systems Owners.

Clock Synchronization

1. All systems clocks shall be synchronized using Network Time Protocol (NTP) to ensure the accuracy of audit logs.
2. Users shall be restricted from changing the systems time.

Patch Management

1. [***IT section/department or the function assigned with responsibilities of IT 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.
2. Prior to deployment of patches in information systems, patches shall be validated and tested including security patches and system upgrade patches.
3. [***System Administrators or the job title assigned with responsibilities of systems administration***] shall ensure that a roll-back plan is identified before deploying any patch.
4. Timelines for patch implementation shall be defined and agreed with the respective information Systems Owners and business owners.
5. [***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).

Wireless Network Security

1. The management and maintenance of Wireless Infrastructure management 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 of configuring the wireless infrastructure as per the Entity Wireless security policy.

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 as per the Entity *Remote Access Policy*.
3. Remote access shall be authenticated using a two-factor authentication mechanism.
4. [***System Administrators or the job title assigned with responsibilities of systems administration***] shall configure remote access in alignment with the Entity Remote Access Policy.

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 administration 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 in 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).

Security Assessment and Vulnerability Management

1. [***Information Security Section/Department or the function assigned with information security***] is responsible for conducting periodic vulnerability assessments and penetration tests on the IT management.
2. [***IT section/department or the function assigned with responsibilities of IT 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.
3. [***IT section/department or the function assigned with responsibilities of IT Management***] shall address the vulnerabilities identified through the security assessments in coordination with [***Information Security Section/Department or the function assigned with information security***].

4. [***IT section/department or the function assigned with responsibilities of IT 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.,
5. The security baseline documents shall be updated periodically to address the latest vulnerabilities.
6. The [***Information Security Section/Department or the function assigned with information security***] shall review and sign-off on the baseline documents.
7. [***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. [***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.

Policy Compliance

1. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

Electronic Communication Usage Policy

Objectives

To ensure information exchanged between authorized resources are secured within and across entity boundaries.

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 compliance to this policy within their area(s) of concern.

Policy in Detail

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 Usage

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 as 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 the 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. A disclaimer and uniformed electronic email signature must be assigned on all outgoing electronic communications and Users are prohibited from altering or removing details related to it.
16. Users shall refrain from sending email attachments that may spread viruses (such as .exe, .bat, .com, .scr, .vbs, .jar etc.).
17. Users shall refrain from configuring automatic forwarding of official emails to non-[***Entity Name***] hosted email system.
18. Official email distribution lists or group mailing lists (where appropriate) shall be created in coordination with responsible section/team of electronic communication systems.

Policy Compliance

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 compliance to this policy within their area(s) of concern.
6. Users shall be aware that the [***Information Security Section/Department or the function assigned with information security responsibilities***] in coordination with the responsible section/team of electronic communication systems reserves the right to monitor all official electronics communication channels to ensure that electronics communication usage is as per this policy.

Health Information and Security Policy

Objectives

The objective of this Policy is to ensure healthcare information are suitably protected by [***Entity Name***] to uphold public trust and reliability on governmental interest and values, and to sustain entity reputation in the provisioning of healthcare services.

Scope

This policy applies to all Health information managed, handled or processed by [***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 compliance to this policy within their area(s) of concern.
6. The [***Director General or job title assigned with responsibilities of Entity's higher management***] of [***Entity Name***] shall endorse this policy for its effective implementation.

Policy in Detail

Health Information Privacy and Protection

1. Orientation shall be conducted on healthcare information protection and sanctions to all employees, relevant contractors and third parties prior to their access to healthcare information.
2. Process shall be established to ensure that access to health information systems and applications are restricted for individuals possessing a valid license to practice their profession within the UAE, and any exception shall be authorized by entity CISO based on adequate justification.
3. Cleaning staff access shall be restricted to areas where patient related healthcare information is being viewed, accessed, used, processed, stored and/or destroyed are monitored or under surveillance coverage.
4. Processes shall be established to notify the health sector regulator of any probabilities of breaches involving healthcare information.

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. Where appropriate these principles are elaborated below to provide the basis by which [***Entity Name***] security will shape the direction and conduct of security:

1. Maintain the confidentiality, integrity & availability of Information & Information assets.
2. Meet the UAE regulatory, statutory and legislative requirements.
3. Report and investigate all suspected breaches of Information Security.
4. Provide appropriate Information Security Training & awareness to all employees (permanent & contract employees).
5. Design appropriate controls and procedures to support the implementation of this Information Security Policy.
6. Ensure all stakeholders are responsible for implementation of respective security policies & procedures within their area of operation, and oversee adherence by their team members.
7. Continually improve Information Security through implementation of corrective and preventive actions.
8. Prepare, maintain and test Business Continuity Plans in a practical manner based on the business needs.
9. Annually review this Policy for adequacy and appropriateness.

Policy Compliance

1. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

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:

- Reduce probabilities of information leakage and loss
- Secure information assets
- Minimize unauthorized access and usage
- Uphold organizational and governmental reputation
- Ensure service continuity

Scope

This policy applies to all Users of [***Entity Name***] and it covers all kinds of information and information processing facilities 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 compliance to this policy within their area(s) of concern.
6. Projects Owners/Projects Managers are responsible for ensuring compliance to this policy.

Policy in Detail

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:
    - Compliance with legal and regulatory requirements.
    - Compliance with Intellectual property rights requirements.
    - Compliance with information security policies and procedures.
    - Clear allocation of responsibilities to all the involved parties.
    - Statement on Non – Disclosure of information.
    - [***Entity Name***]'s rights to review and audit the compliance with the contracts.
    - Adequate Service Level Agreements (SLA), where applicable.

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:
   - Possible impacts to the controls of the information processing facilities;
   - The classification of the information assets;
   - Processes for identifying, authenticating ,authorizing and reviewing access rights of the Third Parties; and
   - Security controls that are in place to control storing, processing, communicating, sharing or exchanging information.
4. All risks identified shall be appropriately addressed through risks mitigation measures.

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 with remote access before obtaining prior approval as per the [***Entity Name***] Remote Access Policy.

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).

Policy Compliance

1. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

Information Systems Acquisition, Development, and Maintenance Security Policy

Objectives

To emphasis the need for healthcare 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.

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.

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 compliance to this policy within their area(s) of concern.
6. Projects Owners/Projects Managers are responsible for ensuring compliance to this policy.

Policy in Detail

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 systems acquired and developed shall be relevant to the business requirements of [***Entity Name***] and shall be supported by business requirement documents.
3. All Information System and Application acquisition initiatives shall be documented and approvals from Head of the sections shall be obtained.

4. 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 Team.
5. Information Systems Security requirements shall reflect the business value of the related Information Assets and the potential damage that may be caused due to absence of protection mechanisms.
6. Information system design documents, addressing the security requirements shall be developed and approved.
7. Security requirements shall include:
    a) User authentication;
    b) Access provisioning and authorization processes, for business users as well as for privileged or technical users;
    c) Informing users and operators of their duties and responsibilities;
    d) Protecting Information Assets as per the Information Classification and Handling Policy;
    e) Business processes specifics, such as event logging and monitoring, non-repudiation required;
    f) Mandatory security controls, e.g. interfaces to logging and monitoring or data leakage detection system.

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.

Policy Compliance

1. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

Information Security Incidents Management Policy

Objectives

To ensure that healthcare 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 applies to all Users of [***Entity Name***]. It covers all type of information security incidents that occurs or suspected to target on any information or information processing facilities owned or managed by [***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 compliance to this policy within their area(s) of concern.

Policy in Detail

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:
   - Detailed description of the information security incident including time of incident.
   - Details of the user(s) who reported the information security incident including contact details.
   - Asset/service affected by the information security incident (or thought to have been affected).

- Damages observed including any other security events/violations occurred.
- Information security Incident status – occurred / ongoing / may occur.
- Details on how the information security incident was discovered/detected.
- Reference of any similar occurrences in the past.
- Supporting evidence.
- Remedial steps taken, if any.
- 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 an Incident Response Team (IRT) for carrying out incident response activities.
5. The IRT 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 IRT shall carry out root cause analysis and take corrective actions to contain and eradicate the incident.
7. 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)
8. Incident shall be monitored from its identification till closure. Based upon the progress, the incident records shall be updated on a continuous basis.
9. 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 in the Security Incident Management Database (SIMDB) for future references.
7. All evidences 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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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

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:

1. Security Incidents Severity

Priority	Alert Level	Activity Description	Impact
P1	Critical (Very High Risk)	Threat of, or actual, malicious cyber activity (hacking, viruses, or other activity) that will disrupt, destroy, or degrade [***Entity Name***] systems and infrastructure. Incident occurred, is imminent, or is ongoing Zero-day exploit has been released and is expected to target [***Entity Name***] systems The incident will seriously impact [***Entity Name***]'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 Name***] Infrastructure and services Potential or observed serious and widespread degradation or destruction, threatening continued operation of [***Entity Name***] 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 a [***Entity Name***] providing a national critical service is present or reported Zero-day exploit has been released The incident affects [***Entity Name***]'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.	Potential for or observed major degradation, disruption and/or destruction of [***Entity Name***] Infrastructure and services Potential for or observed high level of degradation, disruption or 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, focused attack exploiting known vulnerabilities and weaknesses) or expected intrusion activity 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 Name***] 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 Name***] 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

2. SLA Matrix

		Incident Acknowledgement	Incident Resolution	Resolution Notification to DoH SoC
P1 - Critical	SLA	Within 1 hour of incident communication/observation	Within 2 hours of incident communication	Within 2 hours of incident resolution
	Mode of Communication	**Primary:** Email **Secondary:** Phone	**Primary:** Email **Secondary:** Phone	**Primary:** Email **Secondary:** Phone
	Responsible Stakeholder	Help Desk	Technology / Application Owner	Help Desk
P2 – Severe	SLA	Within 1 hour of incident communication/observation	Within 4 hours after the incident is reported	Within 2 hours of incident resolution
	Mode of Communication	**Primary:** Email **Secondary:** Phone	**Primary:** Email **Secondary:** Phone	**Primary:** Email **Secondary:** Phone
	Responsible Stakeholder	Help Desk	Technology / Application Owner	Help Desk
P3 – Elevated	SLA	Within 1 hour of incident communication/observation	Within 24 hours after the incident is reported	Within 8 hours of incident resolution
	Mode of Communication	**Primary:** Email **Secondary:** Phone	**Primary:** Email **Secondary:** Phone	**Primary:** Email **Secondary:** Phone
	Responsible Stakeholder	Help Desk	Technology / Application Owner	Help Desk
P4 - Normal	SLA	Within 1 hour of incident communication/observation	Within 48 hours after the incident is reported	Within 24 hours of incident resolution
	Mode of Communication	**Primary:** Email **Secondary:** Phone	**Primary:** Email **Secondary:** Phone	**Primary:** Email **Secondary:** Phone
	Responsible Stakeholder	Help Desk	Technology / Application Owner	Help Desk

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 applies to all Users of [***Entity Name***], and it covers all [***Entity Name***] IT infrastructure, IT Services, Information Systems, health systems and Non-IT services.

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 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 in Detail

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.

Policy Compliance

1. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

Compliance Policy

Objectives

The objectives of this Policy are:

- ❖ 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.
- ❖ To comply with the applicable UAE laws, Intellectual Property Rights (IPR), contractual obligations with vendors and contractors.

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 compliance to this policy within their area(s) of concern.

Policy in Detail

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:
   - Compliance with legal and regulatory requirements.

- Compliance with Intellectual property rights requirements.
- Compliance with information security policies and procedures.
- Clear allocation of responsibilities to all the involved parties.
- Statement on Non – Disclosure of information.
- [***Entity Name***]'s rights to review and audit the compliance with the contracts.
- 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:
   - Ensuring that software installed and used in [***Entity Name***] systems is strictly in accordance with the applicable licenses conditions.
   - 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.
   - Maintaining records and evidences of procurement and ownership of software licenses.
   - Maintaining an Inventory of all [***Entity Name***]'s assets and identifying the requirements to protect IP rights.
   - 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.
   - Ensuring that [*Entity **Name***] Users are adhering to copyright terms of any external party materials, such as books, articles, documents, movies, etc.
   - Prohibiting [*Entity **Name***] Users from installing or using any pirated and unlicensed software on [*Entity **Name***] equipment or systems.
   - 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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

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 applies to all Users of [***Entity Name***], and it addresses the use of all information and information processing facilities that are required by Users to carry out their daily business activities.

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 compliance to this policy within their area(s) of concern.

Policy in Detail

Acceptable Use of Information

8. Users shall ensure that information regardless of its form (electronic or physical) is classified appropriately to avoid loss of confidentiality & integrity of the information.
9. Users shall ensure that information shall be accessed on a strictly "need to know" basis based upon the classification of information.
10. Users shall refrain from discussing [***The Entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.***] under the following circumstances:
    - 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.

- While using Internet based communication channels such as public forums, blog sites, social networking sites, public mailing list, etc.

11. Users shall not share or send [***The Entity shall specify the classification level of information affected by this control, for example confidential information or internal information or secret, etc.***] outside office premises without prior approval from the Entity's respective higher management or the assigned owner of the information.
12. 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 internal information or secret, etc.***].
13. 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).

Clear Desk & Clear Screen

1. 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.***] whenever leaving the office unattended as detailed in the clear desk & clear screen policy.
2. User shall ensure that any [***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 white boards are wiped off, once the discussion is complete, and shall ensure that such information is not visible from outside the room during the meetings.
3. Users shall ensure that they lock the computer screen whenever leaving their desks.

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 any one 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 Abudhabi 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

5. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with [***Relevant HR Law***], the Code of Conduct for Employees and any other applicable UAE Laws in this regard.
6. 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***].
7. 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.
8. 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.

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 applies to all Users and physical assets (information and computing resources including Desktops, Laptops and Servers) 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 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 in Detail

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:
   - 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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

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 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 compliance to this policy within their area(s) of concern.

Policy in Detail

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. Users shall ensure that they lock the computer screen when leaving their desks.
2. 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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

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

The scope of this policy covers all the information / data stored and processed in production, development, test environments, file servers, as well as network and security devices owned by [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 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 in Detail

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 transfers 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 with a minimum distance of 40 KMs from the onsite location.
5. Offsite backup must be maintained in a fire resistant enclosure and must be covered with appropriate physical security.
6. Access to backup media while onsite, in-transit, or offsite must be restricted.
7. If backup tapes are discovered to be damaged or corrupted, then these tapes must be destroyed.
8. 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 are removed
    - Tapes and others non-reusable data storage media are physically destroyed.
9. 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.
10. 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***].
11. Handling backup media must be done according to the manufacturer's recommendations and guidelines to prevent damage.

Backup 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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

Internet Usage Policy

Objectives

The objectives of this policy are to:

- Ensure efficient and reliable internet usage for all Users in [Entity ***Name***].
- Protect confidential information and intellectual properties belonging to [Entity ***Name***] and ensure that any risk of exposure is minimized.
- 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 compliance to this policy within their area(s) of concern.

Policy in Detail

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:
   - End of employee's service
   - Contractors completing their engagement

- If requested by the Director of the department which the user belongs to.
- 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 non official 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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

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 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 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 in Detail

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 password for all systems/applications
3. Users shall set strong passwords matching the following criteria:
   - Minimum length of password should be eight characters or [***to be decided by the entity based on the risk and business needs***].
   - Should contain a combination of alpha numeric characters and at least one special character.
   - Should contain both upper and lower case characters.

- Not to be repeated within a cycle of 3 passwords changes [***to be decided by the entity based on the risk and business needs***].
- Not to be easily guessable and must not contain:
  - Names of family members, pets, friends etc..,
  - The name of popular places, (i.e. "Abudhabi", "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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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.

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 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 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 in Detail

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:
   - Users who have compelling date to complete tasks/projects.
   - Users working on tasks/projects which requires remote connection after working hours.

- 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:
    - 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.
    - End of employee's service.
    - 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.
    - If Users have not used the Remote Access for 90 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 HR disciplinary procedure in accordance with [***Relevant HR Law***], 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 healthcare 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:

- Information leakage
- Unauthorized access
- System compromise
- Misuse of privilege, facilities and information
- Loss of information
- 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 healthcare entities. The entity's management should apply adequate control measures to address those risks.

<u>The objectives of this domain's controls are:</u>
To ensure that the right 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

<u>HR 1.1 Human Resources Security Policy</u>

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 3.1 to HR 3.4.
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 Department of Health 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 Management Policy
2) Acceptable Usage Policy
3) Compliance Policy
4) Disciplinary Actions Policy

HR 2 Prior to Employment

HR 2.1 Background Verification:

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 Department of Health 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 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 academic qualifications and professional memberships, verification of work 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 health information, financial information or any other highly confidential information, more detailed checks should be done. 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.

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:

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 terms and conditions of employment should typically include:
A. A requirement that employees, contractors, and third-party users who are given access to sensitive information sign a Confidentiality or Non-Disclosure Agreement.
B. The requirement for the employee's, contractor's and third-party user's commitment to copyright laws and data protection legislation
C. The requirement to follow the entity's information classification scheme. All data classified as confidential should be handled, stored and transmitted securely, whether in electronic or paper form.
D. The obligation of the employee, contractor, or third-party to handle information responsibly and their personal accountability for deliberate or avoidable breaches of information security.

E. Disciplinary actions to be taken if the employee, contractor or third-party user violates the entity's information security requirements

The employee, contractor, or third-party should be briefed on the information security requirements of the Employment terms and conditions. The record of this briefing should also be retained along with the signed terms and conditions and signed Confidentiality or Non-Disclosure Agreement as applicable.

HR 3 During Employment

HR 3.1 Establishing Policies and Procedures:

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 and Training: [T]

With cybersecurity as with healthcare, 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. All entity staff subject to Department of Health licensing procedures will in the future also have to undergo Cybersecurity e-learning as part of their CE / CME / CPD process.
Notwithstanding the support from the Department of Health, it is the entity's 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 policies of the entity. The training should be to an annual schedule and a record of awareness training provided should be maintained.

HR 3.3 Skill and Competency Gaps:

Due to the fast digitalization in the field of healthcare there is a situation where the most experienced medical professional may have the least experience with computers and other electronic equipment. This can lead to security and accuracy issues. Security maybe compromised if usernames and passwords are shared with junior staff to help with data entry. On the other hand, wrong data could be entered due to unfamiliarity with the software / keyboard / mouse.

Another example can be staff responsible for entity IT and IT security becoming a security weak point if they have not been provided training to keep up with the changing technologies they manage.

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.

HR 3.4 Awareness campaigns:

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 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 will in the future also have to undergo Cybersecurity e-learning as part of their CE / CME / 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 policies of the entity. The training should be to an annual schedule and a record of awareness training provided should be maintained.

HR 3.5 Disciplinary Process: [T]

A disciplinary process 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:

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

Change of contract should be managed as the termination of the current contract or employment, and the new responsibility should be handled like a new employment.

HR 4.2: Return of Assets

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

Due to the sensitive nature of health 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 Department of Health or Abu Dhabi government to revoke any relevant system and application access upon termination.

HR 4.4 Process to Manage Transfers and Change of Role

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 healthcare Information Security management. Healthcare 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 healthcare 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, healthcare 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:

1. Information (in physical and digital forms)
2. Medical device and equipment
3. Applications and Software
4. Information System
5. Physical Infrastructure (Data centre, access barriers, electrical facilities, HVAC systems, etc)
6. Human resources (in support of care delivery)

<u>The objectives of this domain's controls 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 healthcare entities to monitor and record the use of information assets.

Asset classification is defined in detail in Section A-5 of the ADHICS standard. Personal and patient information should always be classified as Confidential.

For visual representation, DoH Standard classification colors and categories should be used:
Red = Secret
Orange = Confidential
Blue = Restricted
Green = Public

AM 1 Asset Management Policy

AM 1.1. Asset Management Policy

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 Department of Health 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

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

The healthcare 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:

- IT Assets i.e. Laptops, workstations, storage, servers, security devices (firewall, IDS/IPS, anti-spam, etc.)
- Network assets i.e. Routers, gateways, switches, wireless access points, printers etc.
- Staff - Information Technology Director/Manager, Database architect/administrator etc.
- Internal applications - Electronic medical records (EMR), Financial control, ERP, CRM, email etc.
- External facing applications - Websites, Mobile Apps, E-commerce, IP addresses, DNS services, etc.
- Data - Customer personal data, customer health data, entity's employee personal and
- financial data
- Physical facilities - Hospitals, medical centers, clinics, pharmacies, data centers, etc.

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 2.2 Asset Ownership

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:

1. Define/identify the control requirements to minimize the impact of risk, due to the compromise of assets under his/her ownership.
2. Review the adequacy of implemented control measures periodically and amend/modify the control environment as necessary.
3. Ensure effectiveness of the implemented controls, in addressing the risk environment.
4. Authorize access and/or use of information assets.

Note that the patient is the final owner of his/her personal health information and 'Owner' designated by the healthcare 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 2.3 Acceptable Use of Assets

The healthcare entity should establish and enforce rules on the acceptable use of information assets. The Human Resources Security domain has related information under HR 2.2, HR 3.1 and HR 3.2.

1. The rules should be communicated to all employees and contractors in support of care delivery, and should be read and acknowledged by all.
2. Entities should maintain records of user acceptance on the acceptable use of information assets.

The rule 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 2.4 Acceptable Bring Your Own Device Arrangements

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.

Accessing personal health information on personal devices is not recommended without a strong mobile device management (MDM) solution. The MDM should be able to containerize and fully separate entity information from personal information.

1. Probabilities of compromise through the use of personal devices should be addressed through suitable rules and role-based usage agreements.
2. Authorization to use personal devices to access/view/use/share/process/store personal health information is subject to user acknowledgement on the usage agreements.
Control process and technology solution should be implemented to reduce/address/contain factors of risk.

AM 3 Asset Classification & Labelling

AM 3.1 Information Classification

The healthcare entity should classify all information assets, that categorizes information assets into one of the following Department of Health classification schemes:

Red = Secret
Orange = Confidential
Blue = Restricted
Green = Public

The Department of Health standard colors for classification used for visual representation as given above. See also Section A-5 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 personal health 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, 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.

AM 3.2 Value of Information during Classification [T]

Information classification should consider value of the information and should be more restrictive/deterrent based on the entity's tolerance of financial impact due to compromise of the information considered.

The entity should consider the immediate financial impact as well as the costs of any regulatory or legal penalties.

AM 3.3 Identification of Essential Protection [T]

The level of essential protection needed for an asset should be considered while determining asset classification. The classification should be done consistently.

Results of classification should indicate value of assets depending on their sensitivity and criticality to the entity, e.g. in terms of confidentiality, integrity, and availability. The designated 'Owner' should evaluate each item to decide its classification. Besides the financial impact a key criteria can be the presence of personal health information.

AM 3.4 Reclassification of Assets (T)

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

1. Change in the value of information
2. Changes to environment (location, access, storage, processing, usage, etc.)
3. Changes in protection levels

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

AM 3.5 Interpretation of Third Party Classification Scheme (T)

The healthcare 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 Department of Health 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 3.6 Criteria for Automated Classification (A)

The healthcare entity should establish criteria for automated classification of information and should consider using technology solutions to do so based on established classification scheme and criteria.

Automated classification software is available where carefully chosen parameters like keywords allow the software to analyze a document or email and recommend the right template. This is possible for data already on storage as well as documents being generated. The software could force classification of documents while saving or emails when the send button is clicked.

AM 3.7 Asset Labelling

The healthcare entity should establish process to label its information assets in all its form (physical & digital) 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.

Employees and external party users should be made aware of labeling procedures.

Department of Health standard colors for classification should be used such as:
Red = Secret
Orange = Confidential
Blue = Restricted
Green = Public

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

AM 4 Asset Handling

AM 4.1 Handling Procedures

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 he 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.

1. Handling procedures should detail security requirements during:
• Access granting and privilege allocation
• Processing
• Storing
• Communication/sharing
• Printing
2. Security requirements based on asset value should be considered in the handling procedures.

AM 4.2 Enforcement of Handling Procedures

Ensure adoption and application of handling procedures while handling information. Following defined procedures will ensure that handling, processing, storing, and communication of information is consistent with its classification. Any temporary or permanent copies of information should be protected to a level consistent with the protection of the original information

AM 4.3 Management of Removable Media

The healthcare 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 its use must be discouraged at all times. Encryption of data should be considered.

The entity should:
1. Establish media management procedures to address lifecycle requirements (setup, distribution, utilization and disposal)
2. Implement rules and guidelines for protecting assets against unauthorized access, misuse or corruption during movement.

AM 4.4 Usage of Removable Media

Access and usage of removable media should be controlled and should be based on the entity's management approval.

Entity management should:
1. Accept all involved/inherent risk concerning the use of removable media, and should bear all responsibilities and is held accountable for the risks inherent in authorizing the use of removable media.

AM 4.5 Medical Devices Management Procedures

The healthcare entity should establish medical devices and equipment management procedures for each category of identified medical devices and equipment. The procedures should include handling of personal health information on the device where applicable. Secure operation and storage of the devices or equipment should be covered.

AM 4.6 Access Allocation for Medical Devices

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 healthcare entity should:
1. Secure and safe-guard medical devices and equipment in accordance with its classification scheme and risk factor.

AM 4.7 Security of Information within Medical Devices

The healthcare entity should prevent unauthorized disclosure, modification, destruction or loss of patient health information stored on medical devices and equipment.
Entities should ensure that:
1. Information stored within the medical devices and equipment should be encrypted
2. Electronic communication between medical devices and equipment is encrypted
3. Healthcare entities define the minimum essential qualification required to operate and/or handle medical devices and equipment
4. Copies of valuable health data are moved to a secure storage/location to reduce the risk of its data damage or loss.

AM 4.8 Communication Facility for Medical Devices

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 4.9 Removable Media Security [A]

Entity should deploy technology solution to white list 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 4.10 Removal and Movement of Information Assets

The healthcare entity should establish control procedures for the removal, movement, and transfer of information assets (information, equipment, medical devices, and information processing equipment/systems).
Healthcare entities should:;
1. Authorize removal, movement and transfer of information assets. Equipment, information, or software should not be taken off-site without prior authorization
2. Maintain records of removal, movement and transfer for audit purposes.

AM 5 Asset Disposal

AM 5.1 Information Asset Disposal

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

- by the entity
- on basis of regulatory demands or
- for legal proceedings

The retention demands of various healthcare laws and regulations should be followed before physical or digital data is disposed.

AM 5.2 Secure Disposal

The healthcare entity should establish a control process that ensures data once destroyed is not recovered.

Due to the sensitivity of personal health information it is recommended that media 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.

AM 5.3 Disposal of Physical & Digital Media

Media, both digital and physical, when no longer required should be destroyed by the entity.

AM 5.4 Procedures for Secure Disposal and Re-Use (T)

The healthcare entity should establish control procedures for the secure disposal or reuse of media, equipment, devices and systems, containing classified information.
The healthcare entity should:
1. Ensure sensitive data and licensed software has been securely removed beyond recovery, prior to disposal

AM 5.5 Verification before Disposal

Retention requirement of data/information contained within media and system should be verified and complied with, prior to disposal. 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.

AM 5.6 Authorization for 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 a healthcare 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 5.7 Records on Disposal

The healthcare 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:

- Information and/or asset owner
- Type of media
- Classification
- Disposal type
- Reason for disposal
- Retention expiry date (if data)
- Data removal confirmation and evidence
- Disposal authorized by

Domain 3 - Physical and Environmental Security

Information and information processing equipment(s)/facilities has greater dependence on physical environment to achieve business objectives. Physical environment and its security are foundational elements to define secure data processing, data storage, data communication/sharing, data hosting and data disposal. Physical and environmental security programs and efforts define the various measures or controls that protect healthcare 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;

1. Physical protection of data center and information processing equipment(s)/facilities
2. Physical entry control for secure areas
3. Medical devices/equipment(s) protection
4. Heating, ventilation, and air conditioning of critical areas and work places
5. Supporting mechanical and electrical equipment's
6. Surveillance of critical areas and work places
7. Security and protection of physical archives
8. Fire and environmental protection
9. Visitor management

The objectives of this domain's controls are to:

- Ensure that information assets receive adequate physical and environmental protection, and
- 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

The healthcare 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:

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

2. 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

3. Consider classification of information assets and their physical presence
4. Define roles and responsibilities for actions expected out of physical and environmental security policy
5. Be reviewed, updated and maintained at planned intervals or during significant changes to operating or risk environment, whichever is earlier
6. Be read and formally acknowledged by all users
7. 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 1.3 for Medical equipment should also be taken into account while defining this policy.

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, the Department of Health 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

PE 1.2 Procedures and Guidelines for Physical and Environmental Security Policy [T]

In addition to the Physical and Environmental Security Policy, healthcare 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 entity should also ensure that the physical and environmental security policy and all supporting procedures and guidelines are periodically reviewed and updated.

Safety of patients and staff as well as protection of personal health information should be the key criteria for these procedures and guidelines.

Besides emergencies based on hazardous medical equipment and bio-hazards, consideration should be given to any security threats presented by neighboring premises, e.g. a fire in a neighboring building, water leaking from the roof or in floors below ground level, etc.

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 1.3 Medical Devices in Physical and Environmental Security Policy

In addition to normal physical and environment items the Physical and Environmental Policy of a healthcare entity should consider specific needs of medical equipment and devices.

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.

The physical and environmental policy should address processing of personal health information should require any workstations with access to such information to be situated in a way that prevents unintended viewing or access by subjects of care and the public.

Protection of personal health information during maintenance, decommissioning and/ or authorized off-site activities should be covered as well.

PE 2 Secure Areas

PE 2.1 Physical Security Perimeter

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

The healthcare entity should:

1. Identify secure areas, 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.
2. 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.

3. 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.

4. The entity should 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.

5. Information systems managed by the entity should preferably be physically separated from those managed by third parties.

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 health 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

Secure areas involved in information processing and personal health 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:

- Maintain a list of authorized personnel having access to secure areas.
- Authenticate all persons accessing secure areas.

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

- 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.

- 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.

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

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

- 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:

- should be responsible for quarterly monitoring of the records/logs and surveillance footage.
- should also maintain an up to date list of users for the secure area, authorized by the management.
- should also maintain an inventory of physical keys, cards or other access methods including current holder. This list should be kept confidential.

PE 2.5 Secure Office /Meeting Rooms

Offices, meeting rooms and facilities in support of healthcare service delivery should be equipped with adequate physical security measures.

Demarcate and isolate public access areas and key work areas, to restrict public or visitor or customer access to key work areas of the facilities. Medical facilities are a unique environment that patients and staff are often in the same area. This can expose personal health information. Care should be taking during facility design to reduce the risk of staff computer screens being exposed to unauthorized people.

The entity should avoid obvious signs that indicates the type of information or activities in the secure areas if it is area that may handle sensitive information.

PE 2.6 Protection against External & Environmental Threats

The healthcare 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 healthcare entity should ensure that fall-back 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 centre infrastructures.

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

PE 2.7 Adequacy/Effectiveness of Control Measures (T)

The healthcare entity should ensure that physical and environmental protection countermeasures and procedures applied are aligned with the outcome of the Risk Assessment and regulatory mandates.

The primary responsibility of safe healthcare delivery must be achieved to the extent possible.

PE 2.8 Working in Secure Areas

The healthcare entity should design physical protection guidelines for working in secure areas. The guidelines should cover:

- Activities in secure areas. Unsupervised working in secure areas is not allowed for safety and information security reasons.
- Control access of mobile, portable and surveillance devices/equipment/utilities, to secure areas. Any device that can be used to carry out data should be controlled.

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

PE 2.9 Stakeholder Awareness [T]

As covered in HR 3.1, 3.2, and 3.4, employee awareness and acceptance of security requirements and arrangements is critical for success.

All personnel including third parties should be educated not to discuss personal health information in public areas.

Unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities.

PE 2.10 Delivery and Loading Areas

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 healthcare entity’s asset management procedures.

Access procedures for loading and unloading areas should be defined to restrict access only to authorized personnel.

PE 3 Equipment Security

PE 3.1 Equipment Siting and Protection

The healthcare 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 health information with insufficient access control should be sited in a lockable area.

PE 3.2 Supporting Utilities

Stable power and communications is a basic requirement. Therefore, the healthcare entity should protect equipment and medical devices from disruptions caused by failures in supporting utilities.

To ensure uninterrupted power provision to information processing systems and medical equipment, healthcare entities should evaluate and mitigate the associated risks.

For example:

- Power and communications lines into information systems should be protected with no cables exposed to human traffic.
- Power cables should be segregated from communications cables to prevent interference
- There should be controlled access to patch panels, cable rooms, circuit breakers to prevent accidental or intentional misuse;
- Where applicable, electromagnetic shielding should be used to protect cables from interference;
- Scheduled physical inspections to identify deviations as well as unauthorized devices being attached to the cables;
- Provision for UPS and/or power generator where applicable taking into account power load as well as expected runtime.

PE 3.3 Maintenance of Equipment

The healthcare entity should maintain supporting equipment, to ensure their continued availability. This control is applicable to facilities classified as Advanced. The entity should:

- Document the suppliers' recommendations for the maintenance of equipment and make them available to the maintenance personnel. The entity's maintenance staff should be fully aware of the manufacturer's safety requirements as well.

- Establish operating procedures for commissioning, maintenance and decommissioning of equipment activities. These should meet or exceed the requirements of the manufacturer. Equipment being decommissioned must be clear of personal health information.

- Establish maintenance schedule of supporting utilities, and maintain up-to date records for maintenance carried out. Supporting utilities include electricity, telecommunications, water supply, natural gas, sewage, heating, ventilation and air conditioning.

PE 3.4 Cabling Security

As discussed under PE 3.2, stable power and communications is a basic requirement for entity operations. Therefore, the healthcare entity should protect equipment and medical devices from disruptions caused by failures in cables carrying power, telecommunication and cables carrying data.

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

- 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.

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

- The entity should use electromagnetic shielding to protect cables from interference where applicable and should use fibre optic cables for data in areas with high electromagnetic radiation.
- The entity should schedule physical inspections to identify deviations as well as unauthorized devices being attached to the cables

See also CM 5.

PE 3.5 Security of Equipment Off Site (A)

A healthcare 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 healthcare 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 personal health information is allowed to go off-site on the equipment. This is also applicable in case leased equipment is 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 personal health information from outside the entity's facilities.

PE 3.6 Unattended User Equipment

Misuse of unattended systems and equipment introduces a major risk of information leakage and unauthorized activities. This is applicable to IT as well as to medical equipment and devices. Establishing procedures regarding leaving equipment, medical devices and information processing systems unattended is mandated by ADIHCS Standard. In line with this:

- All users should be made aware of these security requirements and their personal responsibility to information security.
- Users should logoff before leaving equipment;
- Automatic logoff after a preset idle time should be implemented wherever supported by the equipment; and
- Equipment without such functionality could be protected by locking the room or the area.

PE 3.7 Clear Desk & Clear Screen Policy

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 can be photocopiers. As such:

- All unnecessary hard copies should be shredded before disposal.
- All employees and contractors should be made aware of their responsibility.
- In secure areas, contractors should not be allowed to use cameras or mobile phones when unsupervised.
- Meeting rooms should be cleared of all confidential data at the end of a meeting.
- The Clear Desk & Clear Screen Policy should be read and acknowledged by all employees and contractors of the healthcare entity

Domain 4 - Access Control

A healthcare entity's ability to provide authorized access and its commitment to control unauthorized access to information and information processing systems under its custody are key elements to demonstrate the entities' objective interest to protect information that belongs to:

- Its customers,
- Patients of the Abu Dhabi healthcare ecosystem,
- The Government, and
- The healthcare entities themselves.

The influence of information on the delivery of healthcare and related services and the increased dependence on application and technology, demands that the avenues and provisions of access are strictly controlled. It is essential that healthcare entities understand the responsibilities concerning access management and are accountable for the consequences arising from breaches or disclosures from their respective areas of authority.
Healthcare entities should define policy mandates and process mechanisms essential to secure and protect their information and information systems. Healthcare entities should take specific care when personal health information is being accessed or used and should define access criteria that conforms to the following facts:

- A healthcare relationship exists between the user and the data subject (the subject of care whose personal health information is being accessed),
- The user is carrying out an activity on behalf of the data subject,
- There is a need for specific data to support care delivery or continuum of care.

The healthcare 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:

- Abu Dhabi Government,
- Abu Dhabi Healthcare-ecosystem or Health Sector,
- Patients concerned, and
- Healthcare entity itself.

<u>The objectives of this domain's controls are:</u>
To ensure access to information and information systems are controlled, and to minimize probabilities of information leakage, tampering, loss and system compromises.

AC 1 Access Control Policy

AC 1.1 Access Control Policy

The healthcare 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 personal 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 personal health 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:
1. Be relevant and appropriate to control and secure access to information, application, technology, medical devices and equipment;
2. Include management demands and directions, scope and specific applicability based on:
    a. Type of service,
    b. Information,
    c. Application,
    d. Technology,
    e. Medical devices and equipment;
3. Emphasize the requirement-of-need and role-based access principles;
4. Establish criteria for access, with core focus on:
    a. granting of access,
    b. access authorization,
    c. access revocation,
    d. access termination;
5. Address the healthcare entity needs on secure password management and practices;
6. Mandate the usage of unique identity and complex password;
7. Where relevant, define control measures and provisions for portable/mobile devices, including user owned devices, that handle the healthcare entity's data or has the healthcare entity application(s) to conduct business transactions;
8. Include control requirements for the access and use of network services;

9. Include management actions on violations and deviations;
10. Define roles and responsibilities for actions expected;
11. Be reviewed, updated and maintained at planned intervals or during significant changes to operating or risk environment, whichever is earlier;
12. Be approved by the entity's top management and should be communicated to all employees and third parties having a role in care delivery;
13. Be read and formally acknowledged by all relevant stakeholders.

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 Department of Health 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) Clear Desk and Clear Screen Policy;
2) Network Access Control Policy;
3) Password Management Policy;
5) Facility Access Control Policy.
The level of applicability of above-mentioned policies will vary depending on the individual healthcare entity.

AC 2 User Access Management

AC 2.1 User Registration and De-Registration

Unique user accounts are mandatory except in equipment that do not support multiple user accounts. 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 setup. 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 temporary 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 2.2 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 healthcare entity's information systems, applications, medical devices and equipment. Identifying and disabling or deleting inactive accounts should also be conducted on a quarterly basis as part of housekeeping.

AC 2.2 Privilege Management [A]

The healthcare 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 a healthcare entity, unauthorized modification or misuse or leaks of personal health information is also a risk.

The healthcare entity should ensure that
1. Normal user accounts are not used as service accounts or used to conduct privileged application and system level activities;
2. "Privilege" or "Administrative" accounts are used by individuals with a role to conduct privilege activities;
3. Users privileges are restrictive in nature, and are assigned based on needs to conduct

business activities;
4. Privilege or administrative accounts are not to be used for conducting normal day to day operational activity;
5. Usage of service accounts are controlled, and are not hardcoded in application codes or scripts;
6. There is multifactor authentication scheme for all administrative access;
7. Mandated administrative or privilege access and associated activities are logged and audited.

AC 2.3 Use and Management of Security Credential

The healthcare 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 eight characters including one number, one upper-case and lower-case character, and a special character. Reusing the last three passwords should not be allowed.

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]

The healthcare entity should protect confidential and secret information on portable or removable media, mobile or portable devices, and medical equipment or devices.

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.

Mobile devices with sensitive information should be managed with a mobile device management (MDM) solution which can enforce encryption as well as device wipe in case of loss.

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

The healthcare 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 equipment. Access should be only for authorized users.

The entity should ensure confidentiality and protection of information during the transmission of personal health information. 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 4 Access Reviews

AC 4.1 Review of User Access Rights

The healthcare entity should review access and privileges granted to its user.

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

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 (white lists)

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

AC 5.2 Remote User Authentication

The healthcare entity should use appropriate authentication methods to control access by remote users. Remote access to a healthcare facility's systems should be provided only in specific cases and should be provided after management approval.

Multifactor authentication should be used with cryptographic techniques. Examples are hardware tokens, machine certificates etc. Dedicated private lines and VPN based solutions could be used.

AC 5.3 Equipment Identification In Network

The healthcare 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 5.4 Remote Diagnostic and Configuration Protection (A)

The healthcare entity should control access for the purpose of diagnostic and configuration. Medical equipment, computer systems, network systems, 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.

The healthcare entity should:

1. Identify and whitelist all ports, services and utilities that are used for troubleshooting, and for diagnostics and configuration purposes.
2. Define protection mechanism for the diagnostic and configuration services and utilities that are essential, and disable services and utilities that are not required.
3. Restrict access for remote troubleshooting, diagnostic and configuration to authorized roles and from authorized workstations.
4. Log all remote access activities related to troubleshooting, diagnostic and configuration.

AC 5.5 Network Connection Control

User access to shared and isolated networks should be restricted. 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. Segregation of networks limits lateral movement of malware if an endpoint is compromised. Medical equipment known to be using unsupported versions should be segregated to ensure that there is no lateral movement of malware in case it is compromised.

See CM 5.3 for info on Segregation in Networks.

The healthcare entity should:
1. Provide access to shared and isolated networks in line with its Access Control Policy, requirements of business applications and need to access shared resources

AC 5.6 Network Routing Control (T)

The healthcare 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 healthcare entity should:
1. Establish processes for secure configuration and rules application for network routing requirements
2. Always ensure source and destination address and services or ports are used while defining and applying routing rules
3. Enable routing protection countermeasures to avoid manipulation of routing systems and tables
4. Define and implement network architecture that segregates and isolates internal and publicly accessible systems.
5. External connections to information systems and networks outside the entity should be managed through interfaces consisting of perimeter protection devices (such as firewalls).
6. Ensure that communications with external systems, networks and key internal systems are always monitored for malicious and suspicious payloads.
7. Periodically scan for any covert channel connections to public networks bypassing entity security defense.

AC 5.7 Wireless Access (T)

The healthcare entity shall ensure wireless access within the entity is secured. See also CM 5.4
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 Wi-Fi. Disable Bluetooth, Wi-Fi and other wireless technologies on medical equipment and devices unless it is being used.

The healthcare entity should:

1. Establish usage restrictions and secure configuration requirements.
2. Establish authorization process for wireless access and usage.
3. Ensure public and guest access are segregated and isolated from the entity's internal network.
4. Ensure that internal wireless is not broadcasted.
5. Authenticate wireless connections using strong encryption mechanism and based on entity's internal authentication scheme.
6. Control privileged and administrative activities are not carried out through the entity's wireless network.
7. Restrict wireless access capabilities of medical equipment and devices.

AC 6 Operating System Access Control

AC 6.1 Secure Log-On Procedures

The healthcare entity should establish and enforce secure log-on and log-off procedures to control access to system and applications.

The healthcare entity should:
1. Ensure that access to entities systems, applications and services that process, use or store healthcare information are authenticated.
2. Enforce automated locking of workstation/system after a predefined period of inactivity.
3. Establish authorization procedures, based on classification of systems, application, services and information in scope.
4. Establish and enforce idle session time-out requirements.
5. Automatically terminate inactive sessions after a predefined period of session inactivity.
6. 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

The healthcare entity should create unique identifier (user ID) for each users 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 6.3 Use of System Utilities [A]

The healthcare 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 block access. A particular case is Windows Powershell where the Powershell 5 supports logging. It is recommended to uninstall earlier versions and allow restricted access Powershell 5 to administrator users only.

The healthcare entity should:
1. Identify essential system utilities and tools and enforce appropriate controls for use
2. Provide access to system utilities and tools based on appropriate authorization
3. Maintain inventory of access to system utilities and tools
4. Monitor use of system utilities and tools

AC 7 Application and Information Access Control

AC 7.1 Information Access Restriction

The healthcare entity should restrict access to information and application system functions in accordance with the access control policy.

Access to information and application access should be restricted and based on need-to-know principles and appropriate authorization. Staff that are not involved in healthcare delivery to the patient should not have access to healthcare data. Eg. Cleaning staff.

Role based access control will allow access based on responsibilities without creating undue delay in healthcare delivery.

AC 7.2 Sensitive System Isolation [T]

The healthcare entity should isolate sensitive systems in a dedicated environment.

Security should be appropriate and proportionate to the value of and degree of reliance on the system and to the severity, probability and extent of potential harm.
Any workstations allowing access to personal health information should be placed in a way that prevents unintended viewing or access by subjects of care and the public. A screen privacy filter can also be evaluated for this situation.

AC 7.3 Publicly Accessible Content [T]

The healthcare entity should implement controls and should not expose non-public information to the general public.

Any entity information that is published, for example, through websites or mobile application must have prior management approval. The process to be followed before information is made public should be documented. Information should be sanitized to remove any personal health information.

The healthcare entity should:
1. Establish and enforce procedures for publishing of public information to ensure non-public information is not exposed accidently or deliberately
2. Establish and enforce procedure to periodically validate that non-public information is not exposed to the public domain
3. Validate relevance of publicly available information
4. Ensure no healthcare and related data is exposed to the public domain

Domain 5 - Operations Management

Healthcare entities continual effort to sustain and improve risk environment demands the need for effective management of operational activities in support of information handling, processing, sharing and storage. Operations management aims to establish and/or strengthen healthcare entities processes and efforts to improve and enhance control environment. Objective outcome of effective operations management includes, but is not limited to:

1. Improved security and reduce probabilities of compromise
2. Reduced errors
3. Controlled unauthorized activities
4. Regulated efforts
5. Increased efficiency
6. Reduced security incidents

The objectivity of providing healthcare services should consider security and safety of assets (data, technology, and application) in support of service delivery and healthcare entities should demonstrate commitment in defining and controlling of operational activities concerning service delivery.

The objectives of this domain's controls are:

To ensure that activities concerning support and maintenance of data, technology, and application are controlled and carried out in a standardized manner to reduce probabilities of errors and compromises, and to increase efficiency and security.

OM 1 Operations Management Policy

OM 1.1 Operations Management Policy

The healthcare entity should develop, enforce and maintain an operations management policy to ensure support and maintenance activities concerning data, technology and application are controlled.

The policy should:

1. Be relevant and appropriate to the healthcare entity's operational and risk environment concerning data, technology and application

2. Establish management demands on:

a. Segregation of duties
b. Configuration management
c. Change control
d. Baselines and minimum security configurations
e. Standard operating procedures
f. Capacity management
g. System acceptance
h. Malware control
i. Quality management
j. Backup management
k. Logging and monitoring
l. Patch management

3. 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 Department of Health 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) Quality Management Policy
5) Backup Policy
6) Monitoring Policy

OM 2 Operational Procedures

OM 2.1 Baseline Configuration [T]

The healthcare entity should develop and enforce baseline and recommended configuration settings for common information technology products and applications, medical devices and equipment.

The healthcare entity, while developing baseline and recommended configuration setting, should consider:
1. 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.
2. Requirements of this Standard – Any setting which conflicts with the ADHICS standard should be changed e.g. Cloud connectivity. Any deviations should be approved and documented.
3. 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.
4. Risk mitigation strategies – Based on risks identified in the risk assessment.
5. Corrective and preventive actions – Mitigations based on audit, assessment and incident outcomes.

OM 2.2 Documented Operating Procedure [T]

The healthcare entity should document 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 stakeholders 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.

OM 2.3 Change Management [T]

The healthcare 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 healthcare entity should:

1. Establish a Change Advisory Board to authorize changes
2. Define and enforce a change management process that addresses the following elements:
   a. Identification and recording of significant changes
   b. Planning and testing of changes
   c. Assessment of potential impacts
   d. Formal approval procedure
   e. Communication of change to all relevant stakeholders
   f. Roll-back plan to be utilized during unsuccessful changes
   g. Post implementation assessment
   h. Maintenance of previous version of software, code and configurations
3. Define information systems and applications, medical devices and equipment that should be covered by the Change Management Process

The Change Advisory Board (CAB) should have business and operations representatives. 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.

OM 2.4 Transition of Information Systems and Applications [T]

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 must approve the move from test/development to production. See OM 2.3. A rollback plan must be in place.

OM 2.5 Segregation of Duties [T]

Separation of roles and responsibilities within information systems protects the systems and information from unauthorized modification or misuse. This is critical in the case of personal health information.

If this is not possible then the entity should implement suitable alternative or compensating controls. This could take the form of audit trails or management monitoring of activities.

Even when care is taken that no single person can access, modify, or use assets without authorization or detection, the possibility of collusion exists and should be taken into account.

OM 2.6 Separation of Test, Development and Operational Environment [T]

The healthcare 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 personal health information from production systems must be used in test systems. The change management process should be followed.

The healthcare entity should:

1. Identify the appropriate level of protection between operational, staging, test, and development environments
2. Document and apply clear processes for the transfer of data, information, code, configuration, software and systems between environments
3. Ensure as-is operational data is not used in test environment
4. Restrict usage/migration of test data into operational environment

OM 3 Planning and Acceptance

OM 3.1 Capacity Management [A]

The healthcare entity should identify and document current and future capacity requirements while planning for new information systems and applications.

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 optimisation and data archiving.

OM 3.2 System Acceptance and Testing [T]

The healthcare entity should establish acceptance criteria for new information systems and applications, changes, upgrades and releases, in addition to satisfactory test results

The healthcare entity should:
1. Establish processes for system acceptance, and ensure system acceptance is acknowledged by the relevant authoritative individual. All steps should be documented.
2. 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
3. Ensure testing is never performed on production systems. Valid personal health information should not be used for testing on development systems. Only dummy personal health information may be used.
4. Ensure user profiles (with permissions appropriate for the tasks) used for testing are different from the ones used for operational and development activities
5. 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.

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.

OM 4 Malware Protection

OM 4.1 Controls Against Malware
The healthcare entity should protect its information assets from malware.

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 healthcare entity should:
1. Ensure minimum security configurations is maintained in all information assets, as applicable and as relevant
2. Implement anti-malware and anti-virus protection mechanisms for network and individual information systems (server, workstation, mobile/portable computing devices)
3. Ensure anti-malware and anti-virus protections mechanisms are updated and current
4. Enable real-time protection capabilities
5. Establish and enforce periodic scan schedules

6. Scan removable media for viruses and malware on all occasions when they are connected to information systems
7. Disable auto-run features for removable media on information systems
8. Configure anti-malware and anti-virus protection systems to alert responsible stakeholders on event, incident or anomaly detection
9. Provide ongoing awareness for users on techniques, tactics and procedure to avoid and minimize probabilities of malware and virus attacks

OM 4.2 Gateway Level Protection for Malware

The healthcare 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 healthcare entity should:
1. Deploy gateway level protection for web and email traffic from and to the entity
2. Implement technology that can detect and prevent access to malicious websites or sites from prohibited categories.

OM 5 Backup and Archival

OM 5.1 Backup Management

The healthcare 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. Encryption of backup data should be considered for offsite storage.

The healthcare entity should:
1. Establish backup management process that identifies;
a. Essential and critical information in support of care delivery, business and entity operations
b. Data owner
c. Data recovery point and time requirements
d. Backup frequencies, time of execution and methods
e. Data restoration frequencies and test criteria

2. Ensure backup of all identified essential and critical data
3. Ensure data restoration requirements for continuity and recovery are adequately met

OM 5.2 Archival Requirements [A]

The healthcare entity should establish data archival requirements that satisfies entities retention demands

Archiving demands are based on the regulations and laws covering the

The healthcare entity should:
1. Establish formal processes for archival and destruction of data
2. Identify data-sets and establish retention requirements as needed by law, regulation, and entity demands
3. Identify and enforce archival criteria (what and when to archive, how long to archive) and methods (physical/electronic) that satisfies established retention timelines
4. Preserve data during archival
5. Destroy data that has crossed retention timelines and are no longer required by the entity
6. Maintain adequate record on archival and destruction

OM 6 Monitoring and Logging

OM 6.1 Monitoring Procedures(Advanced)
The healthcare entity should establish and enforce monitoring procedures for information systems and application, medical devices and equipment

Monitoring standard activities to build a normal pattern of activity will help identify a variation which needs to be investigated.

Monitoring procedures should:
1. Identify aspects (system use, changes, unauthorized activities, internal processing, exception, information exchange, integration, access, etc.) to be monitored
2. Establish frequency and methods (dashboards, web-link, mobile-app, scheduled tasks, parameter validation, logs, records, manual verification, etc.) of monitoring
3. Establish minimum information gathering requirements for each monitoring activities
4. Define minimum time requirements for maintaining information gathered from monitoring activities
5. Define criteria for alerting and escalation
6. Have defined criteria that quantifies specific outcomes of monitoring as incidents
7. Establish roles for monitoring activities and assign specific responsibilities

OM 6.2 Audit Logging(Advanced)

The healthcare entity should enable audit logs recording administrator, operator and user activities, exceptions and security events. The log should include faults related to information processing and communication

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

The healthcare entity should:
1. Identify all activities to be captured in logs for all hardware devices, equipment, operating systems and applications
2. Identify minimum required information to be logged
3. Define minimum frequency requirements for reviewing each type of log
4. Define minimum time requirements for maintaining each type of log commensurate with legal, regulatory and entity demands
5. Ensure that logs are not tampered with or modified or destroyed
6. Ensure unauthorized access to logs are controlled

OM 6.3 Preservation of Log Information (Advanced)

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 healthcare entity should preserve logs in a centralized log management system
The healthcare entity should:
1. Control access to the centralized log management solution
2. Ensure the centralized log management solution is managed by individuals who do not have

operational role in implementing or maintain information systems or application
3. Retain logs for a period commensurate with legal, regulatory and entity demands on each type of log
4. Define use cases and dashboards based on the entity's needs and industry recommendations, and should consider:
a. System utilization and performance trends
b. Deviation from entity policy and procedures
c. Access control variances and violations
d. Any potential sign of security breach or attack

OM 6.4 Clock Synchronization

The healthcare 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.

OM 6.5 Patch Management

The healthcare entity should define and establish formal procedure for updates 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.

Automated patch management systems are recommended for larger organizations.

The healthcare entity should:
1. Ensure all systems and devices that process or communicate information are patched and protected

2. Define criteria and process for application of standard, urgent and critical patches
3. Ensure all critical security patches are applied as soon as practicable from the date of release.
4. Ensure patches are deployed to a subset of systems or devices to allow testing before deployment to all.
5. Ensure firmware on devices are updated
6. Periodically validate patch status of systems and devices in use

OM 6.6 Information Leakage [T]

The healthcare 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. A central DLP software will give granular control per user. Network data leaks can be over email, cloud based storage etc. Blocking at firewalls, proxies, DLP software are options to secure this.

OM 7 Security Assessment and Vulnerability Management

OM 7.1 Technical Vulnerability Assessment [T]

This control specifies the requirement of a vulnerability assessment of the entity's network infrastructure. This is to be done annually. In case of major changes or addition of a new system / application, a fresh scan maybe required.

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 and the Department of Health, Abu Dhabi's health sector regulator. Secure / encrypted methods will be provided by the DOH for uploading this information.

Periodically follow up on the progress and status of mitigation measures with the appropriate stakeholders and verify the effectiveness and efficiency of mitigation measures

OM 7.2 Security of Assessment Data [T]

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 healthcare entity should ensure that assessment data is not available with third parties engaged to conduct assessments beyond the time of engagement
The healthcare entity should:
1. Ensure that system, network, applications and security related information is shared with third parties when they are on-site
2. 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
3. Ensure that any shared reports are suitably protected through an adequate encryption mechanism.

Domain 6 - Communications

Abu Dhabi Government’s vision towards modernization and enhancement of society and services necessitates sharing of appropriate information with eligible stakeholders within and across entities. Stakeholder utilization of information from within and across entity has influenced decisions, and improved outcomes. It is essential that the communication between various information processing components are provisioned through controlled communication process and channel. It is essential healthcare entities define criteria, rules and controls that secure communication processes, components, interfaces, channels and stakeholders to securely aid human to machine, machine to machine, machine to human and human to human communication to facilitate information exchange.

Risk environment of the connected world demands that an entity’s management be conscious of the current risk environment concerning communication and information exchange, and that it defines proactive measures that should:

1. Secure entities communication infrastructures
2. Ensure information exchange are controlled through formal exchange agreements and controls
3. Ensure information is delivered to right stakeholders or information processing components
4. Minimize probabilities of unauthorized access

<u>The objectives of this domain’s controls are:</u>
To ensure information exchanged between authorized resources are secured within and across entity boundaries.

CM 1 Communications Policy

CM 1.1 Communication Policy

The healthcare entity should develop, enforce and maintain a communications policy, to ensure information in transit and information being exchanged are adequately protected

The policy should include the requirements related to Malaffi.

The policy should:
1. Be relevant and appropriate to the entity's information exchange and communications demands
2. Demonstrate management commitment, objectives and directions
3. Establish management demands on:
a. Protection of communication infrastructure
b. Communication and protection of personal health information
c. Information exchange agreements
d. Integration methods
e. Physical mode of information exchange
f. Electronic and/or online transactions
g. Information exchange within and beyond entity boundaries
h. Business information systems
4. Provide framework to protect information in transit from interception, copying, modification, misrouting, destruction and any other unauthorized activities

Depending on the size and structure of the entity, the Communications 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 Department of Health 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 Communication Policy, this domain has the following supporting or dependent entity policy references:
1) Communication & Operation Management Policy
2) Cryptography Policy
3) Network Access Policy
4) Wireless Access Control Policy
5) Cloud Security Policy

CM 2 Information Exchange

CM 2.1 Information Exchange Procedures [T]

The healthcare 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. Personal health information 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:
1. Include control measures to protect and reduce probabilities of compromise during information exchange and transfer taking into account:
a. Classification and value of information
b. Information exchange and processing environment
c. Stakeholders involved
2. Identify minimum technical standards for packaging and transmission of health information
3. Establish responsibilities and sanctions for actions and deviations
4. Define actions to be taken during issues, incidents and deviations

CM 2.2 Security of Information during Transit

The healthcare entity should ensure that critical and private information is protected while in transit.

Using a second communication channel to send the password or decryption key will ensure that even if one channel is compromised the encrypted data or login credentials are not compromised. This is a simple method to ensure confidentiality of information.

The healthcare entity should:
1. Ensure that user-name and password are communicated using two different communication channels (email and SMS-text, or email and phone, etc.)
2. Encrypt critical information before transferring and sharing encryption/decryption key using a different communication channel

CM 2.3 Secure Practices for Information Sharing

The healthcare 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 healthcare entity should:
1. Protect information that is exchanged within the entity
2. Ensure that information exchanged between entities, and information sharing communities are protected
3. For custom-developed applications, ensure that the exchange or transfer of information between systems and applications uses appropriate interoperability standards
4. Identify and implement security requirements for exchanging information and software with third parties

CM 2.4 Agreements on Information Transfer

The healthcare entity should establish agreements between the entity and external parties for the exchange of information and software.

Any exchange of personal health information and personally identifiable information by a healthcare entity shall be governed by Department of Health regulations. All personal health information generated by the healthcare provider is owned by the patient himself / herself. The healthcare entity should ensure the security of the information. This control defines the topics to be covered in the agreement with the external party. In all cases no personal health information should travel outside the UAE without the explicit approval of the Department of Health. The agreement should also specify what happens to shared data at the termination or expiry of the agreement.

The healthcare entity should, prior to the beginning of exchange of information and software:
1. Brief and agree with the external parties on all security requirements to be included in the agreement
2. Include additional control requirements when exchange of information includes:
a. Personal health information (PHI)
b. Personally identifiable information (PII)
3. Clearly define roles and responsibilities of each party to the agreement
4. Establish non-disclosure agreements for all disclosures between the entity and the external parties
5. Include in the agreements:
a. Definitions of information to be protected
b. Duration of agreement

c. Process for notification of leakage
d. Ownership
e. Right to audit and monitor activities that involve personal health information and personally identifiable information

CM 2.5 External Party Awareness of Security Requirements [T]

The healthcare entity should ensure that external parties involved in the exchange of information and software are aware of the security requirements to be implemented.

Monitoring and audit of the external party may be required to ensure awareness of the security requirements. The security requirements should also be applied to any sub-contractor used by the third party.

The healthcare entity should:
1. Ensure all security requirements formally agreed between the entity and the external parties are implemented and are effective

CM 2.6 Physical Media in Transit

The healthcare 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.

In the UAE, the high ambient temperatures in the summer can easily damage media during transportation. Magnetic media can also be damaged by strong electromagnetic fields and moisture.

The healthcare entity should:
1. Identify and ensure that physical media containing sensitive is classified in accordance with the established classification scheme
2. Ensure that physical media in transit containing sensitive information is protected against:
a. Information disclosure or leakage
b. Loss of information or media
c. Modification
d. Unauthorized access
3. Ensure that physical media in transit containing sensitive information is adequately tracked
4. Utilize trusted entity staff or courier service for transporting media

CM 2.7 Electronic Messaging [T]

The healthcare 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 personal health information should be with the highest safeguards. Patient consent maybe required.

The healthcare entity should:

1. Identify and categorize all means of electronic messaging through which the entity information can be transmitted
2. Define specific control requirements for each identified category of electronic messaging
3. Ensure exchange of information is based on need and are addressed to authorized and legitimate resources
4. Ensure appropriate electronic signatures containing legal disclaimers are used for electronic messaging.

CM 2.8 Business Information System [A]

The healthcare entity should develop, enforce and maintain procedures to secure information transferred across business information systems.

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 should:

1. Identify all points of interconnections and integrations between business information systems and identify the information to be protected
2. Identify adequate security measures to be applied to protect each type of information

CM 3 Electronic Commerce

CM 3.1 Security of Electronic Commerce Services [T]

The healthcare 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.

Healthcare 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. 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.

CM 3.2 Online Transaction

The healthcare 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 3.1, the online financial transaction itself must be secure. The payment gateway and the healthcare entity should comply with all applicable laws and regulations. Always enable any optional security offered by card issuers

The healthcare entity should:
1. Identify all information used in online transactions
2. Identify and implement security measures to protect information used in online transactions
3. Ensure security requirements are agreed and captured in service agreements with partners involved in online transactions

CM 3.3 Publicly Available Information

The healthcare entity should protect information available through the publicly accessible system.

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 personal 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 healthcare entity should:
1. Identify all information available through the publicly accessible system
2. Establish process to publish and maintain information on the publicly accessible systems
3. Ensure information is sanitized and approved before publication
4. Define security measures to publish information on publicly accessible systems

5. Ensures that information available through the publicly accessible system is always available and is protected against unauthorized modification

CM 4 Information Sharing Platforms

CM 4.1 Connectivity to Information Sharing Platforms

The healthcare entity should ensure that connectivity to information sharing platforms is secure and controlled.

Transfer of healthcare information to sharing platforms is strictly regulated by the Department of Health (DoH) based on legal mandates. Prior approval is required. Transfer of healthcare information outside the UAE is normally not allowed.

Connectivity from every healthcare 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 healthcare entity should:
1. Maintain a list of information sharing platforms that the entity connects to and/or operates
2. Determine security requirements for connecting to or release of information into identified information sharing platforms
3. Establish security requirement for accessing entity operated information sharing platforms
4. Develop required capabilities to establish secure connectivity to any required sector, national or international information sharing community

CM 4.2 Restriction on Cloud Environment

The healthcare entity should not use cloud services or infrastructure to store, process or share information that contains health information.

All major Cloud service providers are now operating in the UAE. However, their services are partially or wholly provided out of datacenters outside the UAE. This breaks the basic regulation that it is not permitted to transfer, store or process healthcare data outside the UAE. This is an evolving scenario as national cloud solutions may achieve the required levels of confidentiality, integrity and availability. At the same time global cloud service providers are setting up in-country cloud services to meet regulatory demands.

Contact the Department of Health for guidance on specific use cases.

The healthcare entity should:
1. Ensure that healthcare information is not transmitted outside the UAE
2. Identify and disconnect integration of system that process, store or utilize health information with any of the entity's systems that connect or utilize cloud services

3. Not share identified or de-identified health information with 3rd parties, inclusive of counterparts and partners, unless authorized by the health sector regulator of Abu Dhabi

CM 4.3 Security While Connecting to Information Sharing Platform

The healthcare entity should ensure that access to health information exchange platforms within the UAE is strictly controlled.

The rollout of Malaffi (Abu Dhabi Health Information Exchange) will introduce a paradigm shift to healthcare delivery in Abu Dhabi. The awareness and commitment to information security from the entities being onboarded is critical. The requirements of the DoH Policy on the Abu Dhabi Health Information Exchange dated November 2018 are comprehensive.

The healthcare entity should:
1. Ensure that access to health information exchange platforms are provided to resources with an authorized need and are not misused
2. Periodically validate and verify access requirements to health information exchange platforms
3. Conduct frequent assessments and audits to identify misuse and ensure compliance
4. Report on incidents and misuse to the health information exchange operator and the health sector regulator of Abu Dhabi

CM 5 Network Security Management

CM 5.1 Network Controls

The healthcare 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 diagrams should be maintained showing the interconnections. Documentation should extend to patch panels and network wall sockets.

Current stable firmware should to be in use. Configuration backups of network equipment 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.

The healthcare entity should:
1. Ensure that all network components and interconnections are identified and sufficiently documented, including documentation of updates incorporated via the change management

process
2. Ensure that network documentation includes up to date diagrams
3. Identify threats and vulnerabilities affecting network components and network as a whole
4. Implement specific security controls to mitigate identified vulnerabilities
5. Centralize the management of access control to networking components
6. Ensure that only trusted devices and users can gain access to internal networks
7. Continually monitor implemented controls for their efficiency and effectiveness

CM 5.2 Security Requirements in Network Services

The healthcare entity should identify and enforce security requirements, service levels, and management requirements as part of relevant network services agreements.

Availability of external network connectivity is now critical. Connectivity to Shafafiya (Insurance) and Malaffi (Health Information Exchange) require a secure and stable network service. The impact of the loss of network connectivity should be evaluated in terms of its effect on healthcare delivery.

The healthcare entity should:
1. Specify specific security requirements essential for each of its network services
2. Establish minimum security requirements for each identified service
3. Establish service levels for internal and external network service providers
4. Evaluate service level compliance and report deviation to relevant authorities

CM 5.3 Segregation in Networks

The healthcare entity should segregate physical, logical and wireless networks based on criticality, nature of services and users of the information systems. Though this is a basic control, the design and implementation will vary widely depending on the size of the entity and the complexity of its network topology.

The design should take into account the bandwidth demands as well as the value and classification of the information stored or passing through the segment. 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 healthcare entity should:
1. Establish criteria for network segregation
2. Establish and maintain appropriate network security zones, allowing data flow follow through controlled path
3. Establish minimum and specific security requirements for each of the segregated networks,

zones and resources
4. Periodically evaluate the adequacy of implemented segregation strategy

CM 5.4 Security of Wireless Networks

The healthcare 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. See also AM 4.8. 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. Use of unauthorized equipment like wireless extenders should be blocked. See also AC 5.7 for access restrictions.

Domain 7 - Health Information and Security

Health information has become fundamental to the provision of healthcare services. Healthcare entities generate and utilize healthcare information and establish relations with individuals to give the information a persistent value during its lifecycle of usage and references.

Privacy of health information is a patient's basic right, by law and principles, and should be protected. Healthcare entities should demonstrate care, prudence and determination in protecting healthcare information under their custody, and uphold the public trust placed on them.

With the launch of the Health Information Exchange (Malaffi) in January 2019 each connected Healthcare entity will have access to historic health information of their patients even if they were treated at other facilities in the emirate of Abu Dhabi. This functionality also means that the entity goes through an onboarding process. As part of this process, they have to be compliant to the information security requirements of the DoH Policy on the Abu Dhabi Health Information Exchange dated November 2018.

The specific requirements for Malaffi are not part of the scope of this document. The ADHICS standard sets the overall Health Information and Security baselines for all healthcare entities. However, it is recommended to go through the policy above even if you are not in the Malaffi onboarding process yet.

It is a government mandate that healthcare information be considered as highly classified data element, to be protected through its lifecycle. Healthcare 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

Healthcare entities should consider critical:

- One's physical or mental health conditions or state,
- Clinical decisions and healthcare services provided
- Payments concerning healthcare services provided or envisioned

The objectives of this domain's controls are:

To ensure healthcare information are suitably protected to uphold public trust and reliability on governmental interest and values, and to sustain entity reputation in the provisioning of healthcare services.

HI 1 Health Information Protection Policy

HI 1.1 Health Information Protection Policy

The healthcare entity should develop, enforce and maintain a health information protection policy that ensures management's commitment to protect healthcare information

This policy should be communicated to all persons involved in the processing of personal health information. Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management commitment.

Appropriate technical and organizational measures to protect personal health information should be implemented.

The policy should:
1. Define management requirements on;
a. Criteria for access and acceptable usage
b. Accountability and/or data ownership
c. Healthcare data communication or sharing
2. Mandate the requirements of non-disclosure and confidentiality during and after employment
3. Define government sanctions and legal obligations
4. Include reference to organizational disciplinary process

Depending on the size and structure of the entity, the Health Information and 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 Department of Health 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 Health Information Protection Policy, this domain has the following supporting or dependent entity policy references:
1) Information Security Management Policy
2) Acceptable Usage Policy
3) Compliance Policy
4) Disciplinary Actions Policy

HI2 Health Information Privacy and Protection

HI 2.1 Security of Healthcare Information

The healthcare entity should ensure that healthcare information under its custody is suitably protected.

The Federal Law No. (2) for the year 2019 on the use of Information and Communications Technology (ICT) in Healthcare mandates security and safety of health information while also specifying hefty penalties for non-conformance. A combination of staff awareness and strict implementation of entity procedures will improve health information security.

The DOH Policy on the Abu Dhabi Health Information Exchange specifies the following timelines for notification of breaches. Affected individual(s) (in this case, a patient) must be notified of a breach without undue delay but in no event later than 60 days from discovery. Notify the DOH of any breach as soon as reasonably practicable after determining that a Breach occurred, but in any event within 5 Business Days.

The healthcare entity should:
1. Conduct orientation on healthcare information protection and sanctions to all its employees, relevant contractors and third parties prior to their access to healthcare information
2. Establish stricter process to ensure clear desk and clear screen practices are adhered to in areas where healthcare information is used, processed or handled
3. Define and enforce criteria for healthcare information access
4. Ensure access to health information systems and applications are restricted for individuals possessing a valid license to practice their profession within the UAE, and any exception should be authorized by entity CISO based on adequate justification
5. Control and restrict privileges for printing and sharing of healthcare information
6. Ensure cleaning staff access to areas where patient related healthcare information is being viewed, accessed, used, processed, stored and/or destroyed are monitored or under surveillance coverage
7. Ensure any hardcopy/media containing healthcare information is shredded after its usefulness
8. Establish processes for shredding all hardcopy documents before their disposal
9. Ensure that healthcare information with personal identifiers is not available unattended
10. Ensure printing of healthcare information is limited to local printers and are not printed through uncontrolled network printers
11. Establish processes to notify the health sector regulator of any probabilities of breaches involving healthcare information.

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.

Healthcare entity management should be cognizant of the fact that a significant portion of privacy breaches originates with organizations 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 healthcare entities and the government. Entities that entrust access to third parties acknowledge and share responsibilities for the breaches.

A healthcare 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:

1. Reduce probabilities of information leakage and loss
2. Secure information assets
3. Minimize unauthorized access and usage
4. Uphold organizational and governmental reputation
5. Ensure service continuity

The objectives of this domain's controls are:

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

The healthcare 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:

1. Be relevant and appropriate to the relationship of the entity and the third party
2. Establish a framework that facilitates:
a. Secure management of third party services and their role in healthcare and/or related services
b. Defining and including information security objectives
c. Third party briefing of security requirements
d. Definition of roles and responsibilities
3. Demonstrate management's commitment, objectives and directions
4. Establish management's expectations on:
a. Privacy and protection of information assets
b. Access to system, application, device, equipment and critical area
c. Non disclosures and terms of use

5. 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 Department of Health 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

The healthcare entity should identify and enforce security requirements, service levels and management requirements as part of relevant third party services agreements.

The healthcare entity should:
1. Ensure that specific security requirements essential for each of type of services are included in the service delivery agreement
2. Establish minimum security requirements for each identified service
3. Ensure measures and minimum baselines for each of the identified security requirements are established and monitored
4. Establish service levels for each of the service through third parties
5. Define and document the type of information that third party service provider needs access to
6. Assign responsibility for managing third party relationships to an individual or service management team
7. Identify and include Right-to-Audit terms specific to the provisions and environment of service management
8. 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 [T]

The healthcare 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 health information.

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

The healthcare entity should:

1. Monitor compliance of security requirements identified in agreements with third parties
2. Monitor third party services and ensure required reports are received and reviewed by qualified entity resource
3. Implement controls for monitoring the exchange of information between various parties to ensure security compliance
4. Manage incidents and contingencies associated with access and violations
5. Assess and manage business, commercial, financial and legal risk associated with third party services
6. 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 healthcare 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.

Healthcare entity management should identify the relevant 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. Healthcare entity management should be aware of the fact that the solution or the product selected will probably introduce new risks that should managed through their lifecycles.

Based on detailed assessment and entity risk appetite, the healthcare entity's management should choose from one of the below options:

1. In-house development, maintenance and support of application and systems
2. Outsource the development, maintenance and support of application and systems
3. Out-of-shelf product deployment, maintained and support by the vendor
4. Cloud-based application utilization
5. Hybrid approach for the development, maintenance and support requirements

Of these any cloud-based option is not acceptable when any personal health information or other personally identifiable information is to be stored or processed. The Department of Health 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.

The objectives of this domain's controls are:

To emphasis the need for healthcare 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

The healthcare 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 healthcare entities.

The policy should:

1. Be relevant and appropriate to the model and relationship of the entity and involved internal and external stakeholders
2. Demonstrate management's commitment, objectives and directions
3. Establish a framework that facilitates:
a. Defining and including information security objectives
b. Selection of the right model and approach
c. Identification and mitigation of risks in involved business and application processes
d. Definition of roles and responsibilities
4. Establish management expectations on:
a. Privacy and protection of information assets
b. Secure design, development, testing, deployment, maintenance and support
c. Secure access to systems, applications, devices, and equipment
d. Secure processing and communication of information and data
e. Non-disclosures requirements
f. Cryptographic controls and requirements
5. 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 Department of Health 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

The healthcare 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:
1. Be relevant to be used for new information systems or enhancements to existing information systems
2. Be approved by individuals authorized to do so on behalf of business and information security
3. Be compliant with the requirements of this standard and secure coding practices
4. Address all risk elements identified during risk assessments
5. Outline validation criteria to verify control efficiency and effectiveness
6. Define system acceptance criteria
7. Be included and maintained in business and technical requirement documents

SA 2.2 Developer Training

The healthcare 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 healthcare entity should:
1. Identify baseline training requirements that are essential to the developer
2. Acknowledge that developer(s) received relevant baseline training prior to their involvement in development activities
3. Identify training requirements based on implemented security functions and features
4. Design and execute training programs to address additional and future security requirements

5. Include training requirement in agreements, when the requirements are delivered and managed by third parties

SA 3 Correct Processing in Applications

SA 3.1 Input Data Validation

The healthcare entity should validate data input to applications to ensure that the data is correct and appropriate.

Due to the criticality of data that is handled in a healthcare facility, input data validation should be implemented 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 healthcare entity should:
1. Define criteria, rules and validation parameters to validate data input into applications
2. Develop or configure applications to drop input data that is identified as incorrect or inappropriate

SA 3.2 Control of Internal Processing

The healthcare entity should incorporate validation checks into applications to detect any corruption of information through processing errors or deliberate acts.

It is important to note that inappropriate or incorrect changes to the processing of personal health information can have disastrous consequences for patient care and safety.

Validation of data should happen within program modules. Processing errors and system failures should be not result in inaccurate or corrupted information. Programs processing in sequence should wait for the previous process to complete.

The healthcare entity should:
1. Establish minimum requirements for validation checks on internal processing of application under development to ensure correct processing of data
2. Require application developers to provide evidence of compliance with minimum requirements
3. Ensure that the incorporated validation checks are valid and relevant over a period of time and meet minimum requirements through the applications' lifecycles

SA 3.3 Message Integrity

The healthcare entity should ensure the authenticity and integrity of messages in applications

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 healthcare entity should:
1. Identify and enforce requirements to ensure authenticity and integrity of messages transmitted between systems and applications

SA 3.4 Output Data Validation

The healthcare entity should validate data output from applications to ensure that data is correct and appropriate.

In a healthcare entity it is imperative that the patient identification and health information retrieved is accurate. If there is a mismatch in the identification or the health 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 3.5 Off-line Processing Capabilities

The healthcare 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:
1. Include off-line and duplicate or out-of-sequence response message handling capabilities.

SA 4 Cryptographic Controls

SA 4.1 Key Management

The healthcare entity should establish key management to support the entity's use of cryptographic techniques.

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.

Healthcare entities should:
1. Establish process to:
a. Securely generate and use cryptographic keys
b. Revoke/block keys
c. Repair damage or corrupted keys
2. Define standards for:
a. Key strength for various environments
b. Key storage
3. Protect secret and private keys against unauthorized use and disclosures

SA 5 Security of System Files

SA 5.1 Control of Operational Software

The healthcare 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 healthcare entity should:
1. Ensure software installations are carried out only by authorized resources
2. Keep a copy of all software installed, including any previous versions
3. Ensure software installed in production systems are subject to entity change management process and approval

SA 5.2 Protection of System Test Data

The healthcare entity should protect system test data.

Protecting personal health information is of the highest importance. Any test environment does not need real personal data. The use of dummy data should be preferred. Deidentified data and anonymised data can still be a risk. Sanitise test data from all systems. Keep a record of all test data.

The healthcare entity should:
1. Use sample data sets to test application, business and security functionalities
2. 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
3. Maintain records of copying, using and erasing of operational information in test environment
4. Ensure that personally identifiable information is not used as test data
5. Erase any data from test applications immediately after completion of the test

SA 5.3 Access Control to Program Source Code

The healthcare entity should restrict access to program source code

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 healthcare entity should:
1. Ensure that access to program source code is strictly based on need and is in compliance with entity access control policy

SA 6 Outsourced Software Development

SA 6.1 Outsourced Software Development

The healthcare 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 healthcare entity should:
1. Establish and enforce a secure coding policy
2. Define quality assurance processes
3. Include in the outsourced software development agreement the requirement to comply with:
a. All relevant healthcare entity policies, including information security and quality related policies, requirements and functionalities
b. Provisions of this Standard
c. Regulatory and legal requirements
d. Industry specific secure coding practices (OWASP)
4. Include in the agreement the right to audit clause
5. Conduct source code review to identify potential vulnerabilities, back-door and malicious code
6. Control the number, rotation and termination of staff involved in outsourced development activities to restrict:

a. Unauthorized access
b. Leakage of information

SA 7 Supply Chain Management

SA 7.1 Supply Chain Protection Strategy

The healthcare entity should develop a comprehensive information security strategy against supply chain threats to the information systems and application, medical devices and equipment

The healthcare 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 healthcare entity should:
1. Define policy to regulate the acquisition of products and services
2. Limit sharing of configuration and architecture with suppliers
3. Define system acceptance criteria for all new system purchase
4. Ensure product compliance with entity information security requirements
5. Include in the contract:
a. Right-to-Audit clause
b. Non-disclosure requirements
c. Terms to comply with entity information security policy and requirements
d. Terms to comply with relevant federal and local government requirements

SA 7.2 Supplier Reviews

The healthcare entity should conduct supplier review prior to entering into contractual agreement to acquire information systems, medical devices and system/devices components or information system services.

Supplier evaluation should include a check on their commitment to information security. If they use sub-contractors evaluate how they enforce information security to these suppliers.

The healthcare entity should:
1. Define an evaluation process for suppliers of information systems, system components, medical devices and services
2. Periodically review supplier compliance to terms of the agreement and evaluation

requirements
3. Include federal and local government requirements as part of supplier review

SA 7.3 Limitation of Harm

The healthcare entity should identify and limit harm from potential adversaries targeting the entity's supply chain. 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 must be contractually bound to this requirement. In the bidding phase minimum information should be shared besides the actual scope of work.

The healthcare entity should:
1. Limit information sharing with suppliers
2. When essential, share securely relevant and needed information through secure channel
3. Engage with a diverse set of suppliers for critical products and services

SA 7.4 Supply Chain Operation Security

The healthcare 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 must be contractually bound to this requirement. In the bidding phase minimum information should be shared besides the actual scope of work.

The healthcare entity should:
1. Evaluate risks to its information systems, medical devices, services and support operations
2. Agree with suppliers of systems, applications, medical devices equipment, etc.-related products/services on control measures and include them in the supplier contract

SA 7.5 Reliable Delivery of Items and Services

The healthcare entity should 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

Using manufacturer or vendor authorized suppliers and legally licensed software reduces the risk of back-doors or other compromises. Verify vendors standing with the manufacturers where necessary. 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.

The healthcare entity should:
1. Ensure information systems, system components, and medical devices are genuine and are satisfying system acceptance requirements
2. Ensure software delivered has not been altered or modified

SA 7.6 Process to Address Weakness or deficiency

The healthcare 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 healthcare entity should:
1. Identify and document supply chain elements and their interdependencies
2. Identify and address issues concerning supply chain elements
3. Conduct regular assessments and audits of supply chain elements

SA 7.7 Supply of Critical Information System Component

The healthcare 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 healthcare entity should:
1. Establish contingency plans for the supply of any critical information systems, medical devices and system/devices components
2. Consider stockpiling of essential and critical spare components
3. Utilize multiple suppliers for critical components

Domain 10 - Information Security Incident Management

It is the entity management's responsibility to ensure the organization proactively prevents information security breaches and responds appropriately to incidents or near misses.
As the value of healthcare information has grown exponentially worldwide it has become a soft target for malicious intent communities, individuals and nation states. They attempt to disrupt an organization'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. Healthcare entities' 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.

A healthcare entity's ability to quickly and confidently respond to and restore service after disruption attempts shows the entity management's commitment to its vision and objective values towards service delivery. Healthcare entity's 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 Healthcare CERT, which is the 24/7 security operations center of the Department of Health is available in Section 1 of this document.

Objective:
To ensure that healthcare 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.

IM 1 Information Security Incident Policy

IM 1.1 Information Security Incident Management Policy

The healthcare 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:
1. Be relevant and appropriate to the entity's operation and risk environment
2. Demonstrate management commitment, objectives and directions

3. Establish incident management roles and responsibilities
4. Establish a proactive, collaborative and sustainable process of identifying and resolving adverse information security incidents.
5. Establish management demands on:
a. Incident identification
b. Incident response
c. Incident notification/communication
d. Learning from incident
6. 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 Department of Health 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 Security Incident 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) Third party security policy
5) Compliance Policy

IM 2 Incident Management and Improvements

IM 2.1 Incident Response Process

The healthcare 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 personal health information or the loss of availability of health information systems, where such a loss adversely affects healthcare delivery or results in adverse clinical events.

The process(es) should:
1. Have tested procedures to handle incident situations before, during and after the occurrence

of the incident
2. Plan for incident communication to affected stakeholders and relevant authorities. Contact information for the Abu Dhabi Healthcare CERT, which is the 24/7 security operations center of the Department of Health is available in Section A of this document.
3. Management approval on plans and procedures

IM 2.2 Computer Security Incident Response Team

The healthcare 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 healthcare entity should:
1. Establish CSIRT organization with adequate authority, essential roles and responsibilities
2. Identify and nominate competent resources for each identified role of the CSIRT
3. Establish communication and response protocols
4. Allocate adequate funds for CSIRT operations
5. The entity CSIRT should coordinate with its counterparts within the health sector regulator of Abu Dhabi for incidents which will have significant/severe impact on the entity's assets or operations
6. Ensure that significant/severe impact incidents are reported to the health sector regulator of Abu Dhabi
7. Provide suitable training to members of the CSIRT to cover:
a. Past incidents and lessons learnt
b. Current threat environment of the entity
c. New threats and attack trends across the world

IM 2.3 Incident Classification

The healthcare entity should assess and classify information security incidents.
A suggested Information Security Incidents Classification scheme is provided as an appendix to the template for the Information Security Incidents Management Policy provided in Section A of this document. Classification of incidents will help prioritize the response.

The healthcare entity should:
1. Establish an incident classification scheme in line with the recommendations of the health sector regulator of Abu Dhabi
2. Define workflows to handle incidents of various classifications/severity

IM 2.4 Incident Response Testing

The healthcare 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 healthcare entity should:
1. Develop test procedures to validate the effectiveness of its incident response capabilities
2. Establish the expected outcome of test and compare test results to identify gaps
3. Modify process and procedures to address gaps identified

IM 2.5 Incident Records

The healthcare 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 healthcare entity should:
1. Identify all relevant data and evidence to be collected during and after realization of an information security incident
2. Establish procedures for collecting evidence taking into account the:
a. Chain of custody
b. Safety of evidence
c. Safety of personnel
d. Roles and responsibilities of personnel involved
e. Competency of the personnel
f. Documentation
g. Briefing
h. Other identified requirements
3. Preserve documents, records and evidences in compliance with the entity’s retention policy

IM 2.6 Learning from Information Security Incident

The healthcare entity should institutionalize the learning from information security incidents
The healthcare entity should:
1. Ensure lessons learnt from past information security incidents are maintained and shared with relevant stakeholders to aid in:
a. Addressing future information security incidents
b. Minimizing the recurrence of such incidents
2. Build knowledge database on information security incident diagnosis and response

Additionally, the Department of Health will be collecting Information Security incident details from the healthcare entities and sharing relevant incident information back to the sector to minimize such incidents.

IM 3 Information Security Events and Weakness Reporting

I
M 3.1 Situational Awareness

The healthcare 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 Department of Health 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 the Department of Health to reduce the risk exposure across the Abu Dhabi Healthcare sector. These initiatives have been branded as the Abu Dhabi Healthcare CERT.

The healthcare entity should:
1. Identify priority information and share it internally to build the entity’s business model based-context
2. Ensure all identified cybersecurity information is relevant to the:
a. Entity’s business operations
b. Entity’s information system and application, medical devices and equipment
c. Entity’s processes and control environment
d. Entity’s risk environment
3. Establish and coordinate with the healthcare sector regulator of Abu Dhabi to receive relevant cybersecurity information

IM 3.2 Reporting Information Security Events

The healthcare entity should report information security events through appropriate management channels

Early identification and mitigation of security events in healthcare entities will enhance reliable healthcare delivery. The Department of Health will collect, analyze and disseminate relevant advisories to all sector entities. Contact information for the Abu Dhabi Healthcare CERT, which is the 24/7 security operations center of the Department of Health is available in Section A of this document.

The healthcare entity should:
1. Establish a formal channel for entities and external stakeholders to report information security events
2. Ensure all employees and third parties are aware of the need for reporting of information security events and breaches
3. Assign designated points of contact for information security events
4. Establish information security event reporting procedures
5. Establish information security event communication and reporting protocol to relevant stakeholders and authorities (including the healthcare sector regulator)

IM 3.3 Reporting Security Weakness

The healthcare entity should report observed or suspected information security weaknesses in systems or application services (inclusive of medical devices and equipment)

Early identification and mitigation of security weaknesses in health information systems and equipment will result in more reliable healthcare delivery. The Department of Health will collect, analyze and disseminate relevant advisories to all sector entities.

The healthcare entity should;
1. Establish a formal channel for entities and external stakeholders to report information security weakness as soon as they are identified. Having a defined reporting procedure ensures speed in responding to an identified security weakness in order to prevent information security incidents.
2. Ensure all employees and third parties are aware of the need for reporting of information security weakness.
3. Ensure no user exploits information security weakness. User awareness training should include refraining from testing for a suspected weakness. Testing can cause unintentional system failures and the user will be liable.

Domain 11 - Information Systems Continuity Management

Information systems and applications have become fundamental to a modern medical facility's operations. The ability of a healthcare entity's systems and applications to support identified critical services and processes in adverse conditions is a measure of the maturity of the healthcare entity's operational capabilities.

Though the organization's Business Continuity process identifies the availability demand on systems and applications, it is relevant for information systems teams of healthcare entities to align with such process to establish system, application and resource requirements concerning critical services and processes.

Healthcare entities should be proactive in identifying threat scenarios that may impact their information systems and application environment, and devise strategies and plans to ensure system, application and resource availability to support service continuity of identified critical services.

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, and but also for the cross-training of health personnel.

SC 1.1, which defines the requirement for an Information Systems Continuity Management policy is applicable to Transitional and Advanced entities. The remaining controls of this domain are applicable for Advanced facilities only.

<u>The objectives of this domain's controls are:</u>
To ensure systems, applications and resources are available to support service continuity requirements of identified critical services and processes during abnormal situations or environment.

SC 1 Information Systems Continuity Management Policy

<u>SC 1.1 Information Systems Continuity Management Policy</u>

The healthcare 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:
1. 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 facility will also impact the public depending on their services. Also take into account that in case of a disease outbreak or other major incident, staff may also be affected.

2. 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
3. Establish roles and responsibilities of involved stakeholders. More than one person should be required for each. Consider cross-training staff for redundancy.
4. Establish management expectations on:
a. Planning for information system and application continuity during adverse situations
b. Compliance with organizational business continuity plans
c. Testing of continuity and restoration plans
5. Be read and acknowledged by involved internal and external stakeholders. Awareness is once again key to successful implementation.

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 Department of Health 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) Entity Business Continuity Policy
2) Entity Business Continuity/Recovery Plan
3) Operations Management Policy
4) Communications Policy
5) Compliance Policy

SC 2 Information Systems Continuity Planning

SC 2.1 Developing Information System and Application Continuity Plans

The healthcare entity should develop information systems and application continuity plans that should prevent or minimize interruptions to critical business services and processes during adverse situations.

Prioritize critical systems based on Risk Assessment. The information systems and application continuity plans should align with the organization’s business continuity plans.

Continuity planning in healthcare is complicated by the possibility of medical emergencies like disease outbreaks which can affect personnel availability.

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:

1. Identify information systems, processes and information supporting critical business services and processes
2. Be harmonized and support organizational business continuity planning and/or disaster recovery demands.
3. Identify individuals with assigned roles and responsibilities, along with necessary contact information
4. Define call tree matrix and escalation matrix
5. Defined criteria and conditions for plan activation
6. Have provisions to address information security incident-based scenarios and provide guidance to operate and support critical business services during such scenarios

SC 2.2 Implementing Information System and Application Continuity Plans

The healthcare entity should implement the established information system and application continuity plans

Once the plans are finalized, procedures have to be developed and fine-tuned ready for plan activation.
Relevant staff should be trained on these procedures. The entity management should commit to any costs related to the business continuity plan implementation.

The healthcare entity should:

1. Ensure that the capabilities and requirements of the information system and application continuity plans are established and available to be used during plan activation

SC 2.3 Testing, Maintaining and Reassessing Plans

The healthcare entity should test, reassess and maintain its information systems and application continuity plans.

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 healthcare entity should:
1. Define schedules and test information system and application continuity plans to ensure:
a. Adequacy and effectiveness of the plans
b. The entity and resource readiness to execute the plans
2. Document test outcomes and lessons learned
3. Assess plan adequacy during changes to business services, systems and applications
4. Update and maintain information system and application continuity plans based on lessons learned and assessment outcome

Section 5 – Useful Forms & Templates

This section contains templates which are specific to the procedures defined for certain policies.

#	Function	Form
1	New User creation	Click here to download
2	Mailbox request	
3	Folder access request	
4	Application access request	
5	Third party (vendor) user creation	
6	Employee separation	Click here to download
7	Backup Request	Click here to download
8	Third party pre-engagement risk assessment	Click here to download
9	Third party risk assessment	Click here to download
10	Incident Management	Click here to download
11	Corrective & Preventive Action (CAPA)	Click here to download

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.

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:

- Identify non-conformities with requirements of ADHICS;
- Verify conformance to the relevant legislation or regulations requirements;
- Verify conformance to the identified information security requirements in the entity;
- Verify that the applicable ADHICS controls have been implemented and maintained effectively;
- 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:

- Corrective actions to eliminate the cause of non-conformity with the control requirements in order to prevent recurrence;
- 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:

- Ensure that management reviews the ISMS;
- Specify the continuous suitability, adequacy and effectiveness of the ISMS;
- Identify major risks for non-compliance;
- Assess opportunities for improvement;
- Identify the need for changes to the ISMS, including information security policy and information security objectives;

- 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 & Reporting

This section describes the requirements for monitoring the compliance levels of entities and reporting the same to the Department of Health.

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 the initial tool for ADHICS compliance monitoring. This checklist includes all 162 controls and their sub-controls. Entities need to provide documentary evidence for any control they classify as ‘Not Applicable’ to their facility.

An external audit on compliance to the ADHICS standard will be integrated into the existing health facility audit program from 2020 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 from 2020.

Detailed information on these compliance initiatives will be published as they are implemented.

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 – Checklists

This section consists of selected check lists which will be helpful in the verification of the compliance requirements for different domains or functions.

General Checklist

□ Information Security Governance committee established.

□ Information Security roles defined.

□ Information Security roles assigned.

□ Registered domain for web and email.

□ Corporate security policy developed and published.

□ Information security scope defined.

□ All devices containing Personal Health Information [PHI] are inventoried and can be accounted for.

Password Checklist

□ Policies are in place prescribing password practices for the organization.

□ 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.

□ Physical access to secure areas is limited to authorized individuals.

□ Computers running EHR systems are shielded from unauthorized viewing.

□ Equipment located in high-traffic or less secure areas is physically secured.

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 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.

□ Every backup run is tested for its ability to restore the data accurately.

□ 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.

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.

□ 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.