GOVERNMENT OF DUBAI

DUBAI HEALTH AUTHORITY

NABIDH

Unifying Dubai’s Healthcare

Policies and Standards

September 2020 (v1.0)

SECTION 8: Information Security Standards

1. Purpose

1.1. To provide advice about procedures and technical standards that need to be incorporated in an information security policy

1.2. To set out minimum requirements and desired goals at various levels of health care provider operational complexity and risk.

1.3. To maintain the information's confidentiality, integrity and availability.

1.4. To identify, assess, record, prioritize and manage threats concerning the confidentiality, integrity and availability of the Health Information related physical and logical assets.

Confidentiality:	**Access to PHI is limited to authorized users for approved purposes.**
Integrity:	Data and information are accurate, consistent, authentic and complete. It has been properly created and has not been tampered with, damaged or subject to accidental or unauthorized changes. Information integrity applies to all information, including paper as well as electronic documents.
Availability:	Authorized users' ability to access classified information for authorized purposes at the time they need to do so.

Table 1: Information Security Standards – Purpose

2. Scope

2.1. This standard is concerned with the security of PHI wherever it may exist.

2.2. This document assumes personal PHI will be shared – it does not say what information is to be shared or under what circumstances (e.g., where identifiable PHI is anonymized). Restrictions on information sharing apply to Personally Identifiable Information (PII); PHI that has been anonymized is not necessarily subject to the same sharing restrictions.

2.3. All subject of care-identifiable health care information is classified as per the classification scheme identified by each health care provider as a minimum equivalence to 'Shared-Sensitive' category as per "Law No.26 of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai" and given an equal level of protection unless otherwise classified.

3. Application

3.1. The development and application of specific security policies and procedures to support the organisation is the responsibility of the organisation's management. However, compliance with the HISS framework's Risk management section 18.4 is mandatory

3.2. This standard applies, but is not limited to the healthcare providers integrated with NABIDH.

4. Risk Management

Health care organisations must undertake the following three activities as a minimum to meet their responsibilities in managing Health Information. They must identify and treat risks associated with health and related information and information assets through a detailed study of business processes, in determining threats and vulnerabilities and accordingly apply the appropriate risk treatment plans and controls.

4.1. Risk Assessment Methodology & Planning

4.1.1. Develops a risk assessment methodology that aligns with the requirements of the entity's information security program /management system.

4.1.2. Determines a periodic plan for conducting the risk assessment

4.1.3. Identifies the criteria of acceptable risks as part of the risk assessment

4.1.4. Identifies the scope of the risk assessments involving key stakeholders, around their business processes & respective information assets that will be included in the assessment.

4.1.5. Identifies threats and vulnerabilities in line with risk assessment methodology.

4.1.6. Plans and implements a periodic awareness of the risk assessment program across the entity.

4.2. Risk Assessment

4.1.1. Conducts and maintains a detailed risk assessment in accordance with the approved risk assessment methodology.

4.1.2. Develop and apply policies and procedures to address each of the identified risks

4.1.3. Regularly monitor and report on the performance of the above policies/procedures. This includes reviewing each policy/

procedure for effectiveness and updating the policies/procedures as needed.

4.1.4. In summary, the provision of appropriate effective Health Information security:

a. Is a requirement of management.

b. Must be tailored to the individual requirements and exposures faced by each health care organisation. The HISS provides guidance, ideas and comment to support these tasks.

c. Analyses risks and prioritizes them based on the criticality, in order to set treatment plans and controls.

d. Determines and identifies the acceptable risks in accordance with the risk assessment methodology.

e. Documents the risk assessment results and must get it approved by health care provider's higher management or an Information Security Steering Committee established at par.

4.3. Risk Treatment and Mitigation

4.1.1. Selects the proper risk treatment plans (mitigate, avoid, transfer, etc.) For the identified risks.

4.1.2. Determines and selects the appropriate security operational controls (under operational domains within this document) for mitigating the identified risks.

4.1.3. Signs off and authorizes officially the implementation of the risk mitigations controls.

4.1.4. Performs and implements the mitigation controls for the risks identified.

4.1.5. Reviews and monitors the implemented risk mitigation controls for effectiveness.

4.4. Risk Acceptance

Documents the residual non treated risks with justifications and gets it signed off from the Information Security Steering Committee along with the detailed plan for treatment at a later date.

5. Organization and Control categories

HISHD directs the minimum areas of policy, and associated controls, to be developed and applied by all healthcare services providers before getting on-boarded to NABIDH HIE Platform.

The requirements for each individual security section have been grouped into three organisation compliance categories.

Organization Category	Category Indicator(s)
Essential	The controls outlined in the "**ESSENTIAL**" category are the **absolute minimum**. Compliance with this level is required of all health care (or support) organisations ready to be on boarded to NABIDH
Intermediary	Organisations are required to achieve "**INTERMEDIARY**" level for some or all categories. This is based on the type of data they hold, functions they perform or a heightened level of risk they are exposed to as per the reviewed Risk Assessment performed in line with controls described in section (5).

Enhanced	Organisations are required to achieve “**ENHANCED**” level for some or all categories. This occurs when The type, quality or quantity of data they hold, or functions performed, expose them to a significantly **HIGH** level of risk they are exposed to as per the reviewed Risk Assessment performed in line with controls described in section (5). **Or**, As part of their Continuous Improvement cycle directed towards achieving compliance to HISS.

Table 2: Organization and Control Categories

Organisations are required to attain at least the “Essential” level for each section described as per this standard before getting on boarded to DHA’s NABIDH HIE Platform.

The controls or procedures defined for each section is listed for three types of users/hierarchies for a health care provider’s organization:

Organization Category	**Category Indicator(s)**
Management	Users at this level in an entity, are those, whose primary job responsibility is to monitor activities of subordinates as well as the day to day operations or own the responsibility of overseeing a properly managed and implemented Health Information security program/management system and reviewing risk assessment reports
Administrative	Users responsible for managing/supporting/administering the systems deployed
End Users	The users who are consuming the services and working towards achieving health care provider’s objectives

Table 3: Organization and Control Categories

6. Health Information Security Framework

Health Information security Framework (HISS) is broadly divided in to 3 sections: Applicable Legislative requirements (lists the legal & regulatory requirements the health care provider must comply for operating their facilities in the Emirate of Dubai); Governance, and NABIDH Health Information Security Framework. Details of HISS framework is presented on table below.

Applicable Legislative requirements			
DESC ISR	**HRS Legislations**		
NABIDH Information Security Framework			**Governance**
Organization of Information Security	**Access Control**	**AUDIT** ***(Independent Validation / Verification)***	DHA NABIDH HISS Compliance
• Internal Organization	• User Access control • Business requirements of access control • User responsibilities • System and application access control		
Information Security Policies	**System Acquisition, Development and Maintenance**		HRS Policies
• Management of Information Security	• Security requirements of Information systems • Security in development, support and test processes		
Assets Management	**Information Security Incident Management**		
• Responsibility of Assets • Classification • Handling	• Management of Information security incidents and continuous improvement		
Human Resource Security	**Information Security Aspects Of Business Continuity**		
• Prior to employment • During Employment • Termination/Change	• Information Security continuity • Cyber Resiliency		
Physical & Environmental Security	**Compliance**		

Applicable Legislative requirements		
DESC ISR	**HRS Legislations**	
NABIDH Information Security Framework		**Governance**
• Secure areas • Equipment Security	• Compliance to contractual and Legal requirements • Review of Information security activities	
Communications Security	**Cryptography**	
• Network Security Management • Information Transfer	• Cryptographic controls	
Operations Security	**Supplier Relationship**	
• Operation Procedures and responsibilities • Protection from Malware • Control of Operational software • Backup • Technical vulnerability management	• Information security in Supplier relationships • Supplier service delivery management	
Electronic Bio-Medical Devices	**Mobile Device Working**	
	• Mobile device security • Remote or Teleworking	
	Cloud Computing	
	• Cloud computing controls • Hosted solutions	

Table 4: Health Information Security Framework

6.1. Domains of NABIDH Health Information Security Framework

The framework is subdivided into 17 key domains for the organization of Health Information security that are listed below:

6.1.1. Domain 1: Organization Of Information Security

6.1.2. Domain 2: Information Security Policies

6.1.3. Domain 3: Assets Management

6.1.4. Domain 4: Human Resource Security

6.1.5. Domain 5: Physical & Environmental Security

6.1.6. Domain 6: Communications Security

6.1.7. Domain 7: Operations Security

6.1.8. Domain 8: Access Control

6.1.9. Domain 9: System Acquisition, Development And Maintenance

6.1.10. Domain 10: Information Security Incident Management

6.1.11. Domain 11: Information Security Aspects Of Business Continuity

6.1.12. Domain 12: Audit & Compliance

6.1.13. Domain 13: Cryptography

6.1.14. Domain 14: Supplier Relationship

6.1.15. Domain 15: Mobile Device Working

6.1.16. Domain 16: Electronic Bio-Medical Devices

6.1.17. Domain 17: Cloud Computing

6.1.1. Domain 1: Organization of Information Security

a. Objective

(i) To establish a management framework to develop, initiate and control the implementation and subsequent operation of information security within the HealthCare Facilities.

(ii) To explain/define to all HealthCare Facilities, the responsibility for managing information security requirements needs.

(iii) To make sure all staff will be aware of the security responsibility undertaken by the nominated security officer in the healthcare facility.

b. Policy requirements

HealthCare facilities are required to develop policies in order to research, consider, approve, formally document, audit, regularly review and enforce procedures to address:

(i) Setting the information security roles and responsibilities.

(ii) Segregation of duties

(iii) Contact with external authorities

(iv) Contact with information security interest groups

(v) Information security in business requirements.

c. Procedures

(i) Essential procedures

Responsibility	Procedure description
Management	• Information security officer responsibility is formally assigned. • Practical segregation of duties, requirements and opportunities are identified and applied. • Information security principles are incorporated into business requirements.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 5: Organization of Information Security – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure description
Management	• Establish clear lines of responsibility for information security. • Ensure the information security officer responsibility is not assigned to a position with IT operational responsibilities, such as an IT administrator. • If feasible, the information security officer should report through a risk, compliance or to a Steering Committee, or to other appropriate division of the HealthCare Facilities outside of IT. • The information security officer should understand the HealthCare Facilities's accepted risk tolerance. They should work towards implementing information security requirements that are in line with the accepted risk tolerance, while complying with required legislation, regulation or other requirements. • Detailed segregation of duties requirements and opportunities are identified, applied and monitored. • Maintain appropriate contacts with relevant authorities within the field of information security. • Identify key contacts of certain security and judicial authorities to be contacted in the cases of information security incidents, breaches, etc. • Maintain interactions and/or memberships with information security interest groups, forums and associations, in order to keep up-to-date information in the field of information security.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 6: Organization of Information Security – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure description
Management	The information security officer role is assigned to an executive within the governance/management group, excluding the CIO or equivalent.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 7: Organization of Information Security – Enhanced Procedures

6.1.2. Domain 2: Information Security Policies

a. Objective

To set the strategic direction for information security in HealthCare Facilities through documented information security policies.

b. Policy requirements

Information security policies have to address requirements created by:

(i) HealthCare Facilities strategy.

(ii) Regulations, legislation and contracts.

(iii) Current and projected information security threat environment.

(iv) Some consolidation of policies may be warranted depending on the mix of individual organizational security risks and requirements.

c. Procedures

(i) Essential procedures

Responsibility	Procedure description
Management	• HealthCare Facilities must have an information security policy to meet the needs of their organisation, that is reviewed and updated at least annually and/or along with any changes that the HealthCare Facilities might undergo. • The information security policy must address security principles, security responsibilities, and an 'acceptable use policy' for protecting any organisation technology equipment, systems, resources and data. • An information security policy document must be approved by management and published, reviewed and communicated regularly to all employees and relevant external parties.
Administrative	Ensure that all employees and relevant external parties are aware of the information security policy and kept informed of any changes and updates.
End Users	Read, understand and follow obligations under the information security policy.

Table 8: Information Security Policies – Essential Procedures

(ii) Enhanced procedures

Responsibility	Procedure description
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 9: Information Security Policies – Enhanced Procedures

6.1.3. Domain 3: Assets Management

a. Objective

(i) Identify assets belonging to the HealthCare Facilities and define and allocate responsibilities for the protection of these assets.

(ii) Ensure assets receive protection based on their importance to the HealthCare Facilities.

(iii) Ensure assets are continuously maintained to an appropriate security baseline that minimizes their vulnerabilities and threat exposure, such as regular patching and other activities (see also 18.6.1.7. – Domain 7: Operations Security).

(iv) Prevent unauthorized disclosure, modification or destruction of information stored on assets.

(v) Ensure assets are controlled and managed in accordance with best industry practice.

b. Policy requirements

A suitable high-level policy will consider and address at least:

(i) Responsibility for assets.

(ii) Asset classification and declassification in terms of legal requirements, value, criticality and sensitivity.

(iii) Asset storage, handling and secure disposal.

c. Procedures

(i) Essential procedures

Responsibility	Procedure Description
Management	*Responsibility for assets* • Create an inventory of information and information processing assets. • Assign ownership and custodianship of assets as they are created or transferred to the HealthCare Facilities. • Identify and document rules for the acceptable use of information and information processing assets including usage of personal devices in HealthCare Facilities's environment. • The termination process must be formalised to include the return of all HealthCare Facilities's assets issued, both physical and electronic. • Establish procedures to interpret classification labels from other organisations where information is shared. *Asset classification* • An asset classification scheme is to be provided. • Create a set of procedures for labelling information and its related assets in physical and electronic format. *Information assets handling* • Establish procedures for the storing, handling, distribution limitation and secure disposal of information and its related assets in physical and electronic format. • Identify and document a set of rules and guidelines for protecting assets against unauthorised access, misuse or corruption. • Establish procedures for the management of removable media.
Administrative	*Responsibility for assets* • Ensure assets are inventoried and classified. • Periodically review access restrictions and classification of assets. • Inform employees and external parties of the security requirements relating to the assets they use. • Control unauthorised copying/printing of information. • Add access restrictions supporting the protection requirements based on the classification of information. • Create and retain a formal record of authorised recipients of assets. • Protect both temporary and permanent copies of information. • Information assets need to be stored in a secure storage/location to reduce the risk of its data damage or loss as per their classification *Asset classification* • Label assets in accordance with predetermined and approved labelling procedures. *Information asset handling*

Responsibility	Procedure Description
	- Encrypt confidential data on removable media. - Ensure physical assets are sanitised (have information fully removed) prior to disposal. Paper or other physical media must be physically destroyed. - Log and sanitise or destroy media containing sensitive information when it is no longer needed. - Implement rules and guidelines for protecting assets against unauthorised access, misuse or corruption.
End Users	*Responsibility for assets* - Conform to acceptable use policy governing the acceptable use of information and assets including usage of personal devices in HealthCare Facilities's environment. - Justify access to personal Health Information . - Ensure data is classified correctly - Return all organisational assets on termination of employment, contract or agreement.

Table 10: Assets Management – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure Description
Management	Identify, document and manage the asset/assets' lifecycle. (see also 18.6.1.7. – Domain 7: Operations Security)
Administrative	- Ensure to initiate the disposal process once the retention period is reached for the assets. - Store IT assets in accordance with specifications from manufacturers. - Prevent the use of media containing classified information with a system that has a security classification lower than that of the media. - Check information storage to ensure any Health Information and software is rendered non-retrievable prior to disposal or re-use.
End Users	No additional requirements in this section

Table 11: Assets Management – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure description
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 12: Assets Management – Enhanced Procedures

6.1.4. Domain 4: Human Resource Security

a. Objective

(i) To ensure employees, contractors and third-party users conform to the HealthCare Facilities's information security policy and procedures.

(ii) To ensure subject of care PHI are maintained confidentially and securely by those authorised to use it.

b. Policy requirements

All human resource policies and procedures, including relevant contractual terms and conditions, must incorporate information security requirements.

All employees, contractors and outsourced employees are aware of their obligations towards information security and that their roles and responsibilities are defined in relation to securing HealthCare Facilities's information and its processing facilities.

c. Procedures

(i) Essential procedures

Responsibility	Procedure Description
Management	Define security roles and responsibilities of employees, contractors, temporary staff and outsourced employees in alignment with the HealthCare Facilities high-level information security policy. ***Screen new staff*** Define background verification and screening process for new employees, temporary staff, outsourced employees and contractors according to the applicable laws and policies of Dubai Government in relation to their appointed task. ***Contracts & job descriptions*** • Include information security responsibilities and non-disclosure agreements in job descriptions, contracts of employment and contracts for service, and induction material. • Ensure all users receive relevant information security awareness training. ***Termination or change of employment*** Ensure adequate knowledge transfer and job handover. ***Disciplinary process*** Introduce, communicate and maintain a formal disciplinary process for employees, temporary staffs, contractors and outsourced employees responsible for information security breaches.
Administrative	• Follow documented recruiting and termination procedures for creating and removing users' access rights. • Ensure that a user's access rights are regularly reviewed and amended accordingly on changes of role and/or accountabilities within the organisation. • Ensure the return of all equipment and removal of all information security permissions on termination of employment or service contract, or on request. ***Maintain security policy documentation*** • Ensure the organisation has documentation matching current security legislative and policy requirements. • Ensure a security policy responsibility agreement is signed by all employees and contractors. ***Disciplinary Process***

Responsibility	Procedure Description
	Maintain necessary records on the security breaches and the disciplinary action taken by the management.
End Users	***During Employment*** - Act in accordance with all relevant information security policies and procedures. - Be aware of how to report an information security incident. ***Sign security policy responsibility agreement*** At the time of engagement, personnel sign a security policy responsibility agreement to show they have read, understood and accepted the information security policy. ***Exit procedures*** - Return all related assets (including hardware, software, information processing and storage devices, printed material or other hard copies) when leaving the organisation or role. - Transfer and document important knowledge about ongoing operations to the organisation during the notice period of termination. -

Table 13: Human Resource Security – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure Description
Management	- Consider segregation of duties in HealthCare Facilities roles and responsibilities to avoid conflicts. - Ensure all parties receive regular and appropriate information security awareness education and training relevant to their job. - Authorise all role membership additions and changes, and associated information security permissions prior to implementation.
Administrative	- Implement and monitor segregation of duties in the roles and responsibilities of the HealthCare Facilities. - Conduct regular information security awareness training to all parties.
End Users	No additional requirements in this section

Table 14: Human Resource Security – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure Description
Management	No additional requirements in this section
Administrative	• Ensure users have received relevant PHI security awareness training before they are provided with any information security access rights and credentials. • Periodically review the system audit trail of new users and users with recently re-assigned security roles.
End Users	Ensure personnel attend an induction course, which covers information security awareness, education and training relevant to their position accountabilities.

Table 15: Human Resource Security – Enhanced Procedures

6.1.5. Domain 5: Physical & Environmental Security

a. Objective

Prevent unauthorised physical or electronic access to the HealthCare Facilities's information assets and information processing facilities. This will guard against loss, damage, theft, interference or compromise of assets, and interruption to the organisation's operations.

b. Policy requirements

This policy will consider and address:

- Securing areas containing sensitive information
- Protection from environmental threats

c. Procedures

(i) Essential procedures

Responsibility	Procedure Description
Management	• Define security parameters and mechanisms on offices, data centers, and other working areas, based on criticality of such areas. • Provides employees with proper guidelines and awareness on the implemented protection controls in the working areas. • Secure areas that contain Health Information and information processing facilities by restricting or supervising physical access. • HealthCare Facilities must have controlled room(s) to hold critical computer equipment (servers, network). • Ensure there are adequate locks on all access doors. Maintain a record of who has access. • Preauthorize off-site use of equipment, software or information. • Provide secure offices, rooms and facilities and reasonable protection against damage from fire, flood, earthquake or other forms of environmental hazard. • Provide proper maintenance procedures on all information processing facilities.
Administrative	• Protect the perimeters of buildings or sites containing information processing facilities against unauthorized access using suitable control mechanism. • Implement UPS (uninterruptable power supply) systems to avoid power failures where deemed necessary. • Implement maintenance procedures for information processing facilities. • Install fire alarm system and test them regularly. • Implement and monitor closed circuit television (CCTV/surveillance camera) in identified secure areas.
End Users	• Conform to the implemented guidelines in securing work areas. • Do not leave the information assets unattended. • Do not discuss personal Health Information in a place where unauthorized users may overhear it. • Work in a secure area when necessary for the task in hand. • When working off-site, at home or in other public areas, use of portable computers and storage media must be operated in reference to section 22 - Domain 15: Mobile Device Working.

Table 16: Physical & Environmental Security – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure description
Management	• Establish and operate a staffed reception area or other means to control physical access to the site or building. • Establish physical barriers to prevent unauthorized physical access and environmental contamination. • Make provision for private areas where sensitive information can be discussed. • All employees, contractors and external parties must be required to wear a visible form of identification. Any unescorted visitors and/or anyone not wearing visible identification must be immediately reported to security personnel. • All fire doors on a security perimeter must be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional and national standards. They must operate in accordance with the local fire code in a failsafe manner. • Maintain and monitor a secure physical logbook or electronic audit trail of all physical access.
Administrative	• Access rights to secure areas must be regularly reviewed and issues taken to management for action. • Control and monitor access to restricted areas electronically, e.g., via card system or camera. • Conduct proper testing and assessment periodically over all implemented environmental and physical protection controls.
End Users	Report broken or malfunctioning equipment to management.

Table 17: Physical & Environmental Security – intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure description
Management	Information processing facilities managed by the HealthCare Facilities must be physically separated from those managed by external parties.
Administrative	Implement proper security controls over delivery and loading areas.
End Users	No additional requirements in this section

Table 18: Physical & Environmental Security – Enhanced Procedures

6.1.6. Domain 6: Communications Security

a. Objective

Ensure the information communicated between authorized resources are secured within and across health care providers.

b. Policy requirements

Policies are required to address at least the categories listed below:

(i) **Network Security Policy**

HealthCare Facilities shall formally document:

- Network services to govern the interconnections between its network, critical owned business information systems and other networks and information systems outside its formal boundaries
- The types of systems/devices that are not permitted on the network
- Any other prerequisite requirements that must be met before connection occurs

(ii) **Information Exchange Policy**

HealthCare Facilities shall formally document:

- The minimum technical standards for packaging and transmission of information
- The tools to be used for the transmission of information
- How information exchanged over a network is protected from interception, incorrect routing and/or loss
- How information exchanged physically is protected from unauthorized access, misuse or corruption

- Agreed requirements with external parties, relating to transferred information
- Responsibilities and liabilities in the event of information security incidents
- Classification and labelling for sensitive data
- Use of security controls such as cryptography
- Archival and retention policy for electronic messaging/ emails

(iii) Information protection policy

HealthCare Facilities shall formally document:

- Detection of malware during transmission
- Subject of care data leakage
- Attachment of inappropriate information
- Copying/modification and destruction

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description
Management	**Policies, procedures and standards** • Create policy documents on: o Network Security o Information Exchange o Information Protection • Ensure users: o Are aware of their responsibilities when transmitting information o Know the location of and can access the relevant policies, agreements and procedures • Ensure formal confidentiality or non-disclosure agreements are in place with external parties that has personal Health Information . The agreement(s) must cover vendors/contractors dealing with the recipient organisations and include: o Definitions of information to be protected o Duration of agreement

Responsibility	Procedure Description
	○ Process for notification of leakage ○ Ownership • Ensure formal service level agreements are in place to cover at least the main components that support the network infrastructure. • Ensure all agreements and policies are regularly reviewed at least yearly and updated as required. • Ensure appropriate electronic signatures containing legal disclaimers are used for electronic messaging. • Assign roles and responsibilities for network equipment management. • Ensure adequate/high level of network availability. • Establish process to publish and maintain information on the publicly accessible systems.
Administrative	• Ensure all networking devices default accounts have their passwords changed, and default account names are renamed. • Ensure all networks are sufficiently documented including documentation of updates incorporated via the change management process. • Ensure network documentation includes up to date diagrams. • Ensure access to network services and equipment follow the procedures outlined in reference to section 15 - Domain 8: Access Control. • Ensure the DHA HISS interoperability standards are followed for the exchange of Health Information within and between organisations. • Use appropriate encryption standards (Refer to section 20 - Domain 13: Cryptography), when exchanging Health Information between external parties. • Ensure only trusted devices and users can gain access to internal networks via wireless access. • Enables clock synchronization on all networking devices with agreed reference such as Universal Coordinated Time (UTC) to facilitate forensic analysis, and continuously monitor its accuracy. • Terminates network connections associated with communication sessions as per the entity defined time period of inactivity. • Implement measures to ensure adequate/high level of network availability. • Implement an archival and retention procedure for electronic messaging/ emails.
End Users	• Ensure the classification and labelling for sensitive data while exchanging information. (Refer to section 10 - Domain 3: Asset Management).

Table 19: Communications Security – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description
Management	• Identify the types of communication channels and types of sites that can be used for the different types of information being transmitted.

	• Ensure agreements with third parties have the right to audit and monitor activities that involve information.
Administrative	• Implement technology that can monitor the status of network devices in a secure way. • Implement technology that centralises the management of access control to networking components. • Establish and maintain appropriate network security zones, allowing data flow to follow a controlled path only. • For custom-developed applications, ensure the exchange or transfer of information between systems uses the appropriate interoperability standards. • Ensure network appliances are configured to support the segregation of networks. • Provide the appropriate level of protection to devices and information.
End Users	No additional requirements in this section

Table 20: Communications Security – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	**Procedure Description**
Management	No additional requirements in this section
Administrative	• Document and implement tools to enable the detection and prevention of unauthorised information transfer. • Ensure the communication of personal information such as credentials are not sent via the same mechanism where more than one part exists. For example, send the username via email and the password via text – in both cases suitable encryption is required.
End Users	No additional requirements in this section

Table 21: Communications Security – Enhanced Procedures

6.1.7. Domain 7: Operations Security

a. Objective

(i) To ensure appropriate controls are implemented to protect the operational security and recoverability of the HealthCare Facilities applications and information processing systems.

b. Policy requirements

HealthCare Facilities are required to document a high- level policy considering and addressing the categories listed below:

(i) The HealthCare Facilities’s requirements for the backup of information, software, and systems. This must include the level of protection required for the different categories of systems and the expected retention of the data being protected

(ii) Response Plan to a disaster event and where it sits in the HealthCare Facilities’s business continuity plan

(iii) The removal or upgrade of unsupported legacy software

(iv) Requirements for protection against malicious software such as malware, ransomware etc.

(v) Requirements for the frequency and type of testing of information, software, and

system integrity

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description
Management	• Ensure all systems have documented operating procedures that are made available to all users. • Provide regular awareness for users on the importance of protecting health care providers infrastructure from malware attack, by focusing on avoidable user behaviours. • Develop a formal policy around the installation and use of unauthorised software, and ensure technology and processes are implemented to enforce this policy. • Create an accessible and available operating procedures manual(s) that documents: o Backup and recovery procedures o System restart and recovery procedures o Equipment maintenance functions o Change management o Instructions for handling errors o Management of audit trail and system log information

Responsibility	Procedure Description
	o Management of a security event, including a physical security breach or one associated with a malware or hacking breach • Ensure appropriate operating procedures are created, implemented and maintained to protect documents, removable storage media, printed information and system documentation from unauthorised disclosure, modification, removal and destruction. • Ensure systems are monitored and checked regularly to ensure information system problems are identified and corrected. • Ensure data is adequately backed up and stored in a protected location. • Implements a change management process that must include the following details: o Formal management approval prior to implementation o Plan and test changes before implementation o Assess all potential impacts and risks
Administrative	**Protect information, systems and networks** • Implement anti-malware and anti-virus software on all servers and workstations. Ensure it is kept up to date. • Ensure real-time malware scanning is activated and scheduled scans are run on a regular (e.g., weekly) basis. • Ensure appropriate backups (type and frequency) are implemented for each information software/system. • Ensure the backup process includes type, retention, frequency, protection controls and remote storage. • Control the installation and use of unauthorised software. **Patching/firmware** • Ensure HealthCare Facilities is up to date with current threats and ensuring the correct mitigation is in place. • Ensure all critical security patches are applied as soon as practical from the date of release. **Management, monitoring and alerting** • Implement technology that can detect and prevent access to malicious websites or sites from prohibited categories. • Ensure all systems are sufficiently documented, including documentation of updates that are incorporated via the change management process. **Capacity management** Ensure there is sufficient capacity with information systems to support good system performance and reliability.
End Users	**Report problems** Be aware of the dangers of viruses and malware and report suspicious events to management immediately.

Table 22: Operations Security – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description
Management	**Operations procedures** Track systems and their configuration information in a configuration management database. **Protect information, systems and networks** Ensure a system and software lifecycle policy is defined in accordance with the HealthCare Facilities's risk tolerance profile. **Change management** • Establish and apply a formal process: o To control all changes and appropriately authorise all significant changes to information and information processing systems o For emergency changes when incidents occur • Ensure all change processes are reviewed regularly and updated as required. • Ensure back-out/recovery plans are fully documented, incorporating procedures for when a back-out/recovery is required. • Ensure all assets are registered in an asset management system. The system must be able to dynamically update details regularly using agent software or similar. • Ensure a process exists for the adoption of systems from development or project mode to operational status. This includes the development of formal documentation to enable support of the system to the agreed service levels. **People management** • Segregate access rights to reduce opportunities for misuse of information assets.
Administrative	**Information security** • Provide and maintain the ability to: o Write data to portable storage media in an encrypted format o Securely "wipe" data/information stored on hard disks before their re-use or disposal • Formally document operating procedures, including how to dispose media safely and how to encrypt data on portable media. • Ensure system documentation includes up-to-date diagrams. • Protect information, systems and networks. • Ensure archived or stored data is kept in a secured format that is retrievable. • Ensure adequate backup/restore computing and storage resources are available to recover all critical systems following a major event or media failure. • Implement a configuration control system to track versions/revisions of software implemented and their relevant documentation. • Non-compliance procedures (written exemptions etc.) are invoked only for short term to allow for maintenance and upgrades that will bring systems back into compliance. **Patching/firmware**

Responsibility	Procedure Description
	• Formally assign roles and responsibilities for vulnerability management including vulnerability monitoring, assessment and coordination responsibilities. • Document a formal process that outlines standard and urgent patch application, setting out the criteria that must be met before urgent patching takes place. • Ensure patches are deployed to a subset of devices to allow testing before deployment to all. • Where a vulnerability is known or identified but no patch is currently available, use other alternatives to mitigate risk (such as firewall controls to limit functionality or restrict access), and prevent execution of suspect executable files. • Ensure firmware on devices is updated at least yearly, with a more regular requirement if security vulnerabilities are behind the reason for the update. • Where devices are no longer supported and software updates are not available, a risk assessment must be performed to determine the impact of an incident and the increased vulnerability. **Testing** • Test new versions of software and features before deployment. • Require vendors to produce or show evidence of adequate testing, before deploying new versions and features, or provide on-site test facilities to enable pre-deployment testing to take place. • Develop suitable acceptance test scripts for systems during changes and upgrades to systems. • Document and apply clear processes for the transfer of information/software between test/development and production environments. • Ensure sufficient separation exists between test/development and production environments to reduce the risk of accidental changes to the production systems. • Ensure testing is never performed on production systems. • Ensure different user profiles (with permissions appropriate for the tasks) are used for operating, testing and using systems. • Do not allow development tools or editors to be installed onto production systems. • Regularly validate backups by performing an isolated recovery. **Capacity management** • Ensure critical systems have capacity management procedures. • Enable monitoring of capacity management to ensure performance or function is not affected by insufficient resources • Understand the potential effect of the forward pipeline of projects or expansion that requires resources so capacity can be managed appropriately. • Ensure processes exist to regularly: o Decommission systems that are not required o Optimise databases o Archive data that is not accessed regularly

Responsibility	Procedure Description
	• Ensure that in the event of a failure, sufficient priority and resource allocation is given for production to resume before test/development systems. **Time management** • Enable the ability to synchronise system clock(s) to an agreed accurate time source. • Disable the ability to change time on the local device. **Monitoring and alerting** • Maintain and operate an ability to log and/or alert data integrity faults generated by the system. • Ensure logging is occurring for the following activities: o Changes to system configuration o The activation/deactivation of prevention systems such as malware protection • Deploys adequate logs analysis mechanism and places appropriate actions on faults. • Secures, where appropriate, logging systems and log files against unauthorized changes including alterations, deletions, and renaming of log file contents, dates and time stamps.
End Users	**Protect information** • Ensure physically stored media, in rest or in transfer, is encrypted. • Ensure data is classified correctly so the appropriate retention policy can be applied.

Table 23: Operations Security – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure Description
Management	**Operations policy** • Ensure clear service level agreements are created with the business owner(s) for each category of system/service implemented and operated by the HealthCare Facilities. • Ensure the service level agreements clearly state what constitutes an IT disruptive event for the HealthCare Facilities.
Administrative	**Monitoring/alerting** • Ensure log file information is protected for audit purposes, based on the established log tracking timeframes. • Detect and notify the asset management function of the installation of unauthorised software. • Enable logging of administrator/operator accounts and review regularly. • Perform regular checks to ensure access to systems and networks are secure, for example: penetration tests and vulnerability assessments.
End Users	No additional requirements in this section

Table 24: Operations Security – Enhanced Procedures

6.1.8. Domain 8: Access Control

a. Objective

(i) To Exercise sufficient control over information and therefore prevent unauthorised access.

(ii) To minimize probabilities of information leakage, tampering, loss and system compromises.

(iii) To enable Authorised users to view and process only the information they are entitled in a need to know basis.

b. Policy requirements

The HealthCare Facilities's identity and access management framework or system will define user access controls. The level of access control policy required will vary depending on the individual HealthCare Facilities.

(i) **Document Access Control Policy**

HealthCare Facilities shall formally document the following:

➢ **Category Essential:**

- All users of health systems have uniquely identifiable accounts assigned to them to ensure individual responsibility. Generic accounts can be used to provide access to basic desktop functions, but access to health care and administrative applications require users to logon using their user identifiable accounts
- Standard user access profiles for common job roles within the HealthCare Facilities. Formal authorization process for user

account creation/deletion and access requests/removal (this may be part of the information security policy)

- Access rights based on a ‘least rights’ model and ‘prior to access’ approval. The approver understands what they are granting access to
- Along with terms and conditions of employment, there is a mechanism to ensure users sign an agreement that covers information confidentiality and disclosure
- A process to ensure:
    - Access control policies are regularly reviewed and updated where necessary.
    - Systems and applications that require authentication (as per the access policy) have a secure log-on mechanism in place.
    - Utility programs or tools that may be capable of overriding system and application controls are restricted and tightly controlled.
- Access to all accounts used for handling and management of subject of care-identifiable information, regardless of the device used, are to be restricted to that purpose.

➢ **Category Intermediary**

- Privileged user accounts (administrator rights) are only used for the special activities requiring their use, and not for day-to-day activities or over-ride access

- External support staff are only setup with temporary access rights for a fixed period and their accounts are set to expire at the end of that period.
- External support staff accounts are separated from internal staff accounts for easier identification and management.
- Separate authorization process for the management of system or information, over standard user authorization.
- Ensure:
  - Relevant contractual or legislative obligations are met for the access to data and services, particularly for security requirements
  - Access control policies are regularly reviewed and updated where necessary

- **Category Enhanced**

Ensure there is segregation of the access control roles, so the same person is not performing more than one of these roles – access request, access authorization, access administration.

- **Clear desk and screen policy**

The HealthCare Facilities shall formally document a ‘clear desk and screen’ policy to protect paper and information on computer displays being seen by those who should not have access to the information.

- **Password Policy**

The HealthCare Facilities shall formally document:

- Enforcement of passwords to a required complexity level based on the risk profile of the information they have access to
- Password complexity for privileged accounts (administrator access) that exceeds the password complexity required by standard users
- Enforcement of password changes at regular intervals as required by the information security policy
- Prevention of reuse of previous user passwords for a defined period of time e.g., 13 months
- Enforcement of access lockout after a fixed number of incorrect login attempts
- Enforcement of access control measures (passcode etc.) on mobile devices.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description
Management	***General procedures*** Create policy documents covering: o Access control o Clear desk and screen o Password management ***Audit*** • Undertake regular audits of access logs, especially for privileged accounts. • Ensure all access allocation is documented and traceable. • Have a mechanism to allow verification that the level of access granted is appropriate.
Administrative	***Maintain access rights and password policies*** • Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors. • Ensure users' access rights are appropriate to their task and are authorised to removed or modified upon termination of employment or change of role.

Responsibility	Procedure Description
	• Ensure users are only able to access the resources and services required to carry out their duties. • Ensure access to program source code is restricted. ***Password protection*** Ensure passwords are always secured and protected. ***Secure wireless networks*** Ensure any wireless access points on the internal network are secured. ***Session protection*** • Automatically close down or terminate a session after a fixed time period of user inactivity or provide a locked screensaver option where the user must re-authenticate to unlock the system. • Ensure users cannot disable the locking mechanism.
End Users	***Good password practice*** • Follow good practice in the selection and use of passwords. • Do not share or disclose passwords. • Do not keep a record of passwords using a non-secure method such as on accessible paper, in a standard file or on a mobile device. • Change your password regularly as per the password expiry standard defined in the information security policy or if you have any reason to suspect your password has been compromised/is known. • Change your user passwords when equipment has been returned to you after repair. ***Act responsibly*** • Read, review and understand obligations under the access control policy (such obligations may be included in the user's signed security agreement). • Accept responsibility for all access under their credentials and ensure access related to their duties (and notify if it is not). • Do not leave the computer unlocked while unattended. • Report any security breach to the appropriate stakeholder/team. • Prevent any unintended or unauthorised release of information, particularly from unattended equipment, by terminating active sessions, locking the screen or logging off when finished.

Table 25: Access Control – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description
Management	Extend the access control policy to meet policy requirement under this section.
Administrative	***Secure networks and devices*** • Password-protect and encrypt information on devices used for remote connections, including laptops, mobile devices or portable media. • Support secure access to the network. • Password information must not be communicated to users via unencrypted emails. ***Session logging*** • Configure systems to display the date and time the user last logged in to assist in identifying unauthorised use of their account. • Remove or disable utility programs that are not required. ***Password protection*** Ensure passwords are always hashed and stored in an encrypted format. ***Monitor & audit*** • Monitor for repeated account lockouts. ○ Keep an audit trail of all login attempts to the system – including successful login activity. The log should include at least user identifier, date, time, location, and duration of all user activity within an application (including view-only activity). • Allow viewing and analysis of audit trail activity by approved users. Restrict and record the ability to delete or modify log files. • Regularly review audit trails of access and activity – perform in depth audits and pay special attention to privileged accounts and external parties. ***Access control*** • Develop and operate a procedure to provide and revoke access rights at short notice, to support the requirements of backup resources and others for temporary access. • Access the internet via a firewall or centralised device that monitors use and prevents access to unwanted material. • Maintain a remote and mobile device register. ***Policy notification*** Display a logon banner that requires the user to acknowledge and accept security terms and their responsibilities before granting access to the system.
End Users	***Good password practice*** Do not use the same passwords for personal and work-related purposes. ***Act responsibly*** Comply with section 22 - Domain 15: Mobile Devices Working.

Table 26: Access Control – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure Description
Management	Extend the access control policy to meet policy requirement under this section.
Administrative	***Access control*** - Implement tests for user proximity. The request to access information must be for a record that is, for example, recent in both time (looking at reasonably current information – not 'old') and physical location (nearby geographic information). - Do not disclose system or application identifiers until log-on successful. - Applications must enable control of user access rights at each level of access, e.g. create, read, write, modify, delete and execute. ***Advanced authentication*** - Use multi-factor authentication to control access for remote users. - Where strong authentication requirements are identified, use alternatives to passwords such as biometrics, cryptography, smart cards and tokens. - Minimise access times to high-risk systems to reduce the window of opportunity for unauthorised access.
End Users	Do not use passwords that consist of words included in dictionaries.

Table 27: Access Control – Enhanced Procedures

6.1.9. Domain 9: System Acquisition, Development and Maintenance

a. Objective

(i) To ensure the need for HealthCare Facilities in adopting secure system and software development lifecycle management processes.

(ii) 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.

b. Policy requirements

HealthCare Facilities shall formally document a policy for addressing their requirements for ensuring the security on any in-house developed or external party applications regarding the acquisition, development and management of information systems, including mobile applications.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description
Management	Ensure regular maintenance of all information processing systems.
Administrative	As part of a regular maintenance cycle, apply software patches to application and systems software to manage, remove or reduce security weaknesses.
End Users	***Preserve data integrity*** Systems must have controls to ensure data input validation, checks on the loss of data integrity as a result of processing failures, message integrity and data output validation. ***Testing and test data*** • Test data must be selected carefully, protected and controlled. • System acceptance testing must include the testing of information security requirements. •

Table 28: System Acquisition, Development and Maintenance – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description
Management	***Systems maintenance*** Where an organisation lacks the internal resources to perform systems maintenance, this function must be contracted to an external party. ***Mobile applications*** Scrutinize and assess the risks associated with the terms and conditions of the health care providers of mobile applications that are downloaded from App stores. ***Certification of systems*** • Security requirements must be identified and agreed prior to the development, acquisition and/or implementation of information systems. • Promote the use of cryptography controls to achieve information security where appropriate. • Implements security sign off process to confirm the proper implementation of security controls on all information systems/applications prior to deployment.
Administrative	No additional requirements in this section
End Users	***Cryptographic keys*** Where cryptographic controls are used, keys must be protected against modification, loss, destruction and unauthorised disclosure. ***Preserve data integrity*** Systems must support data integrity audits where messages are traceable and reportable. ***Testing and test data*** • The access control procedures, which apply to operational application systems, must also be applied to test application systems. • The use of operational data containing personally identifiable information (particularly subject of care EID), or any other confidential information, for developer-level testing purposes is not acceptable. • If such information is used for testing purposes (for example in user acceptance test environments which require substantial volumes of data that closely resemble operational data), all sensitive details and content must be protected. • Testing is to be performed in a realistic environment to ensure a system will not introduce vulnerabilities to the HealthCare Facilities's environment and that the tests are reliable.

Table 29: System Acquisition, Development and Maintenance – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure Description
Management	***Certification of systems***

Responsibility	Procedure Description
	Mandate the use of cryptography controls to assist in achieving greater information security.
Administrative	***Preserve data integrity*** Operating system services must be locked down to minimise the risk of vulnerabilities and intrusions.
End Users	***Identify potential security vulnerabilities*** Regularly check reliable sources of information about technical vulnerabilities. ***Software development*** Industry best practices must be followed in all software development projects (whether internal, outsourced or purchased products) for the capture, display, processing, exchange and persistence of sensitive information. In particular: o The use of established code libraries, algorithms and routines to implement security features and counter known threats o Source code control o Technical reviews o Testing – unit, integration, compliance and user acceptance o Documentation – for user, business and technical audiences o Change control and version management o Deployment mechanisms ***Testing and test data*** • Separate authorisation is required each time operational information is copied to a test environment. • Operational information must be erased from a test environment immediately after the testing is complete. • The copying and use of operational information must be logged to provide an audit trail. ***Distributed and mobile applications*** In addition to all standard or normal system design requirements, ensure all distributed and mobile applications are designed with the ability to tolerate communication failure. This includes off-line capabilities and duplicate or out-of-sequence response message handling.

Table 30: System Acquisition, Development and Maintenance – Enhanced Procedures

6.1.10. Domain 10: Information Security Incident Management

a. Objective

(i) To ensure the appropriate tools, processes and procedures are in place to detect, report and manage information security incidents.

➢ An information security incident may be either a security breach or malfunction. A potential security incident may also be a threat or weakness that has been identified, which may have a detrimental impact upon the business.

b. Policy requirements

The HealthCare Facilities have to formally document policies to address at least the categories listed below:

- **Security incidents**
  - Examples of security incidents
  - Roles and responsibilities in security incident reporting
- **Reporting security incidents**
  - Reporting security weaknesses
  - Learning from incidents
  - Disciplinary process
  - Procedures for ensuring staff report recorded security incidents
  - Recording incidents
  - Dealing with minor and major security incidents.
- **Investigations**
  - Types of investigations
  - Procedures for investigating security incidents
  - Conducting investigations.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description
Management	***Incident procedures*** • Establish management responsibilities to ensure procedures for incident management are developed and communicated within HealthCare Facilities and applicable external parties. • Create and maintain procedures for incident logging, response, handling, escalation and recovery. ***Incident notification*** • Ensure all employees and contractors are aware of their responsibilities around reporting information security incidents/events/weaknesses, including whom to report and the location of the applicable policies/procedures. • Notify vendors and/or certifying bodies of failures in system security controls. • Notify all affected parties of the security incident and possible consequences e.g., loss of data integrity. • Report significant information security incidents to NABIDH ***Incident response*** • Respond to reported security events and weaknesses in a quick, effective and orderly manner. • Facilitate protection and collection of evidence related to a security event involving staff disciplinary or legal action. • Develop a policy to handle duress situations.
Administrative	***Monitoring and alerting*** • Log, alert and monitor systems/logs for significant events indicating information security breaches and weaknesses. ***Report events*** • Educate users, contractors and third parties in how to report security incidents. • Report any weaknesses identified and security events as they occur. • Follow instructions from management for recording and monitoring security incidents. ***Incident response*** • Implement business continuity plans if needed. • Record all information about an incident in the appropriate register. • Implement containment processes to ensure security incidents do not spread while they are being addressed. • Once all evidence is collected, use appropriate tools and procedures to restore the environment to a normal operating state.
End Users	***Report events*** Report security events and weaknesses through appropriate channels as quickly as possible and in a confidential manner.

Table 31: Information Security Incident Management – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description
Management	***Assess*** Perform vulnerability assessments to determine where weaknesses may exist, and improvements can be made. ***Incident Notification*** Notify other agencies/departments running similar technologies or who may be at risk to the same threat, if an incident occurs. ***Incident monitoring*** Develop formal event monitoring, reporting and escalation procedures to enable the types and volumes of incidents to be monitored. ***Continual improvement*** Institute a process for continual learning and developing improvements from monitoring and analysis of security incidents. ***Procedures*** Provide an anonymous mechanism for reporting suspected security issues so the person reporting can do so without fear of ramifications. ***Incident analysis*** • Develop a procedure to review any security incidents post event and provide recommendations for avoiding a similar incident in the future. • Implement improvements in process, tools or policies to reduce the likelihood of incident recurrence.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 32: Information Security Incident Management – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure Description
Management	***Tasks*** Create and maintain procedures for the handling and storage of forensic incident evidence. ***Incident analysis*** • Review the information gained from security incidents to determine the cost of each incident. • Review past incidents and lesson learnt.
Administrative	The failure of critical and/or out-of-band patching is to be included in the incident response as an event.
End Users	No additional requirements in this section

Table 33: Information Security Incident Management – Enhanced Procedures

6.1.11. Domain 11: Information Security Aspects of Business Continuity

a. Objective

- To ensure Information security continuity are embedded in the HealthCare Facilities business continuity management systems.
- To ensure availability of information processing facilities.

b. Policy requirements

Policy requirements include identification of:

- An acceptable loss of information security on information and services.
- An acceptable time frame for full recovery of information security.
- Procedures to recover and restore information security.
- The triggers and threats which will cause the business continuity plan to be activated.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	***Information security continuity established*** • Determine requirements for information security and the continuity of information security management in a manner to reduce the impact of major disruptive events. Capture these within the business continuity management process or within the disaster recovery management process. • Establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during a disruptive event. • Verify the established and implemented information security continuity controls at regular intervals to ensure they are valid and effective during disruptive events, i.e., run a restore.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 34: Information Security Aspects of Business Continuity – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure description
Management	***Information security continuity governance***

Responsibility	Procedure description
	• An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event. • Incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated and appointed. ***Information security continuity planning*** Policies are to cover: • All information security aspects of both business continuity and disaster recovery programmes, for example: all related processes, procedures, supporting systems and tools. • Mechanisms to maintain existing information security controls in what may be highly adverse operating conditions. • An ability to operate compensating controls within a known risk. ***Information security continuity plan verification*** HealthCare Facilities must verify their information security management continuity by: • Regularly exercising and testing the: o Functionality of information security continuity processes, procedures and controls to ensure they are consistent with the information security continuity objectives o Knowledge and routine required to operate information security continuity processes, procedures and controls to ensure their performance is consistent with the information security continuity objectives • Reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.
Administrative	***Availability of information processing facilities*** • Information processing facilities must be implemented with redundancy sufficient to meet HealthCare Facilities's availability requirements. • Information restores are tested regularly. • Maintain and regularly check equipment to ensure its continued availability and fitness for purpose.
End Users	No additional requirements in this section

Table 35: Information Security Aspects of Business Continuity – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure description
Management	***Availability of information processing facilities*** • HealthCare Facilities must identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered. • Where applicable, redundant information systems must be tested regularly to ensure the failover from one component to another component works as intended.
Administrative	No additional requirements in this section

End Users	No additional requirements in this section

Table 36: Information Security Aspects of Business Continuity – Enhanced Procedures

6.1.12. Domain 12: Audit & Compliance

a. Objective

(i) To clearly define compliance and audit requirements in order to ensure effectiveness of the implemented information security controls and avoid any violations and breaches to any laws, policies, or controls.

b. Policy requirements

The HealthCare Facilities approach to meeting these requirements must be explicitly identified, documented and kept up to date for each information system.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	• Identify and document all relevant legislative statutory, regulatory, and contractual requirements, and the organisation's approach to meeting these requirements. • Regularly update documentation for each information system and for the HealthCare Facilities. In particular establish procedures to ensure: o Compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of copyrighted/licensed materials, software or applications o Records are protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislative, regulatory, contractual and business requirements o Privacy and protection of personally identifiable information as required in relevant legislation and regulation • Perform regular reviews for the compliance of information processing and procedures relating to the security policies, standards and any other security requirements. • Perform a risk assessment for all information systems periodically, or following significant business or technology

	changes to systems, contract renewals, extensions and/or vendor changes.
Administrative	• Perform regular reviews of information system security operating procedures and practices as directed. • Undertake regular security-related testing activities including but not limited to penetration (vulnerability) testing and disaster recovery testing.
End Users	• Comply with all the applicable policies and contractual agreements. • Report areas of non-compliance to management.

Table 37: Audit & Compliance – Essential Procedures

(ii) Intermediary Procedures

Responsibility	**Procedure description**
Management	Take legal advice on legislative requirements as necessary.
Administrative	Undertake technical compliance review.
End Users	No additional requirements in this section

Table 38: Audit & Compliance – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	**Procedure description**
Management	• Risk assessments applied to all projects/business cases with appropriate approval. • Undertake an independent review of the HealthCare Facilities approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) at planned intervals or when significant changes occur. • Conduct and report on organisational information assets assurance processes regarding security matters (e.g., incidents, responses, issues, risks). This may include undertaking specialist internal/external audits of their environments and taking appropriate action based on findings and recommendations.
Administrative	Implement Information security controls as required by business requirements.
End Users	No additional requirements in this section

Table 39: Audit & Compliance – Enhanced Procedures

6.1.13. Domain 13: Cryptography

a. Objective

(i) Ensure the proper and effective use of cryptography to protect the confidentiality, authenticity, integrity and availability of information using approved cryptographic products, algorithms and protocols.

(ii) Encrypt sensitive information to secure it from outsider and insider threats.

b. Policy Requirements

Cryptographic controls and keys must be protected by policies and procedures that ensure they are implemented, continue to be used, and are decommissioned in a manner that reduces the risks of unauthorised access and misuse.

As part of developing a policy for the use of cryptographic controls, consideration should be given to the selection of appropriate encryption controls. The policy shall include:

(i) Type of Encryption for information transit

(ii) Use of VPN for application-to data connectivity

(iii) Encryption for data at rest

(iv) Consideration of the most current encryption protocols and/or standards in the solution.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	Develops, distributes and maintains a policy on the use of cryptography and key management wherever applicable (e.g. During development and maintenance of information systems/applications etc.).
Administrative	• Implements proper cryptography and key management mechanisms as required by the HealthCare Facilities. • Implements proper protection and security controls on all cryptographic keys used by the HealthCare Facilities. • Keep systems patched and up to date and give priority to critical notifications. • Ensure encryption is enabled on all equipment that is dependent on its own controls to protect itself, such as mobile devices, backups, and offsite storage. • Seek approval for disabling encryption when required for investigative purposes and reinstate encryption when that work is completed. • Do not share passwords and/or access relating to cryptographic keys with unauthorized persons.
End Users	• Report lost and stolen equipment to IT support for appropriate actions to be taken. This action may include remotely wiping or disabling the device. • Comply with any notification requirements from IT support.

Table 40: Cryptography – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure description
Management	• When making new purchases (software, hardware, cloud services etc.) use that time as an opportunity to have vendors and suppliers prove to you their cryptographic products are secure, in that they: ○ Treat equipment to be returned to the supplier for repair, upgrade etc. in a manner that protects any subject of care identifiable information that may still be on it ○ Provide an alert before the expiry of cryptographic keys, to allow adequate time for arrangements to be put in place for their renewal. • People with accountability for cryptographic systems ensure: ○ Security expectations for cryptography and key management are communicated for both new projects and ongoing service delivery ○ Responsibilities are clear and unambiguous for cryptographic systems and key management. This includes responsibility for planning security services that provide oversight for cryptographic systems for the out-years

Responsibility	Procedure description
	○ Contracts comply with cryptographic and key management guidance by preferring solutions that will be upgradeable for the foreseeable system lifetime over one-off point-solutions ○ Recognize that transition periods where legacy cryptography and replacement solutions running side-by-side represent potentially a higher risk than running either solution alone ○ Residual security risks are taken into account when accrediting these systems ○ Equipment used to generate, store and archive keys is physically protected ○ Relevant training and awareness programs are made available for administrators and users.
Administrative	• Manage the distribution and revocation of end-user and system certificates, with a minimum of delay. • Set a minimum notification period for the renewal of any external certificate(s). • Join user groups for the products using cryptographic controls and sign up to automatic notifications and alerts. • Reduce susceptibility to downgrade attacks by removing weak security solutions from selection. Likewise, clear text should only be able to be selected for diagnostic purposes and not operational periods where live data requires protection. Systems are returned to a secure state after running diagnostics. • Implement logging and auditing of key management related activities. • Provide assurance to executive management that cryptographic systems continue to function as intended and that risks continue to be managed and minimized. This may include risk assessments and planning security services for systems for the out-years. • Treat systems used for generating and storing cryptographic keys according to the principles of a higher security classification, as those systems represent potential access to aggregated information and if compromised could undermine the separation of duties.
End Users	• Ensure familiarity with the HealthCare Facilities's policy on the usage of cryptography controls. • Seek advice on encryption from relevant support team when procuring new technology. • Ask to be briefed on encryption and key management arrangements.

Table 41: Cryptography – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure description
Managem*ent*	***Establish and document a cryptographic policy*** • Define how the standards will be implemented throughout the HealthCare Facilities. • Categories the information needing to be protected and assign the relevant encryption standards. • New cryptographic products and services are to be evaluated during procurement to ensure their cryptographic protocols,

	algorithms, key strengths etc. are upgradable over the expected lifetime of the system(s) proposed. This is in response to a changing threat environment, exploitable vulnerabilities being discovered, and as a protection against unintended misconfiguration. • Non-upgradable cryptographic solutions are avoided, except for short lifetime disposable technologies (devices) that can be quickly decommissioned and replaced in response to an event or incident. • Cryptographic key lifetime (e.g., validity start date, validity end date, and validity period) is appropriate and key materials are fit for the renewal cycle. Keys should not normally have a validity period of more than two to three years. • Weak cryptographic capabilities when tolerated in legacy systems (supported by time-bound written exemptions etc.), are improved at the next upgrade. • Development, test and production environments have separate chains of trust to support a separation of duties. • Revoke then replace compromised cryptographic controls (protocols, algorithms and keys) in a timely manner when responding to a security event or incident.
Administrative	Reduce susceptibility to downgrade attacks by ensuring revoked and or weak solutions are not reintroduced as a result of patching and upgrades.
End Users	No additional requirements in this section

Table 42: Cryptography – Enhanced Procedures

6.1.14. Domain 14: Supplier Relationship

a. Objective

(i) To ensure all HealthCare facilities have policies and procedures in place to protect information exposed to third party organizations involved throughout a procurement process agreed upon within contractual agreements.

This section must be read in conjunction with 18.6.1.9. - Domain 9: System Acquisition, Development and Maintenance.

b. Policy requirements

The review and auditing of services against contractual agreements by external suppliers must be informed by the following policies:

(ii) Define and document the criteria for selecting a supplier.

(iii) Assess supplier risks.

(iv) Create a formal contract and confidentiality agreement.

(v) Establish access controls appropriate to the degree of risk identified.

(vi) Monitor compliance with all contractual terms.

(vii) Ensure that all information assets are returned, and all access rights revoked, on the termination of agreements.

(viii) Ensure information is appropriately protected.

(ix) Ensure suppliers reporting for the information security incidents.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	***Supplier relationships*** • Assess and manage business, commercial, financial, security and legal risk associated with suppliers. • Approve potential suppliers based on risk profile. • Mandate security controls to manage risks. ***Supplier agreements*** • Establish and document supplier agreements to clarify the responsibilities of all parties involved in regarding fulfilling information security requirements. • Create appropriate formal service level agreements or equivalent with penalty clauses. • Check implementation of agreements with third-party suppliers, monitor their compliance with information security requirements and manage changes to ensure security controls are operated and maintained properly.
Administrative	***Supplier relationships*** • Assess and manage technical security risks associated with suppliers. • Perform audits of third parties' services on a regular basis. ***Supplier agreements*** • Document incidents where requirements are not met. • Escalate incident reports to administrators and management.

End Users	***Supplier relationships*** Implement controls for the monitoring and auditing of information access. ***Supplier agreements*** Implement controls for monitoring the exchange of information between various parties to ensure agreed requirements are met and any risks that were not covered in the original agreement are highlighted. ***Store audit trail of system access*** Store audit trail of data accessed/modified/deleted by suppliers as necessary.

Table 43: Supplier Relationship – Essential Procedures

(ii) Intermediary Procedures

Responsibility	**Procedure description**
Management	***Supplier relationships*** • Appoint owners for business processes requiring suppliers. • Create a standardised process and lifecycle for managing supplier relationships. • Determine the frequency of audits. • Appoint legal representation to oversee contracts and agreements. • Assign responsibility for managing supplier relationships to an individual within the HealthCare Facilities. (e.g., contracts or commercial manager).
Administrative	***Supplier relationships*** Work with information security, risk, supply/contract management and legal teams within the HealthCare Facilities as required.
End Users	***Supplier relationships*** • Define and document the types of information accessed by different suppliers. • Handle incidents and contingencies associated with supplier access. • Provide resilience, recovery and contingency arrangements to ensure the availability of information for processing. ***Store audit trail of system access*** Monitor and maintain an audit trail of data accessed/modified/deleted by suppliers.

Table 44: Supplier Relationship – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	**Procedure description**
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 45: Supplier Relationship – Enhanced Procedures

6.1.15. Domain 15: Mobile Device Working

a. Objective

(i) To ensure the security of the HealthCare Facilities's information and assets when employees are working outside the office, using mobile devices or when non-organisation devices are used to access the HealthCare Facilities's information.

b. Policy requirements

(ii) **Mobile devices (owned & non-owned)**

The use of mobile and non-organisation owned equipment for organisation business is a growing trend that must only be permitted following the development of clear and unambiguous conditions including rights over the information and images stored.

The mobile device policy must take into account the risks of the use of privately owned mobile devices or bring-your-own-device (BYOD).

Mobile devices must be physically protected. Specific procedures, taking into account legal, insurance and other security requirements of the HealthCare Facilities, must be established for cases of theft or loss of mobile devices. Most important is the protection of the information held on such devices.

(iii) **Teleworking (working outside the office)**

Teleworking refers to all forms of work outside of the office, including non-traditional work environments. This activity is commonly referred to as telecommuting, flexible workplace, remote work and virtual work environments.

A policy for HealthCare Facilities allowing teleworking activities must define the conditions for using teleworking.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	• A policy and supporting security measures must be adopted to manage the risks introduced by using mobile devices and to protect information accessed, processed or stored at teleworking sites. • Training must be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls implemented. • Implement a BYOD policy that addresses the following issues: acceptable use, IT requirements, security requirements (applies to all devices and connections), service policy, ownership of applications on the device, ownership of data/information on the device user, requirements on the employee, lost and found procedures. • Ensure procedure for handling lost or stolen portable computing devices, storage of entity data on these devices, connectivity to HealthCare Facilities network and systems etc.
Administrative	• Implement information security controls for mobile devices in line with those adopted in the fixed use devices (laptops) to address threats raised by their usage out of the office. • Implement a process user must follow in the event of the loss of a device. • Ensure access to equipment, devices, system and facilities at teleworking sites are authenticated, and their access to HealthCare Facilities resources are authorized based on need. • Conduct regular audit of equipment, devices, system and facilities at teleworking sites.
End Users	• Care is to be taken when using mobile devices in public places, meeting rooms and other unprotected areas. • Devices carrying important, sensitive or critical information must not be left unattended and, where possible, must be physically secured.

Table 46: Mobile Device Working – Essential Procedures

(ii) Intermediary Procedures

Responsibility	**Procedure description**
Management	• Institute a policy on the implementation of mobile device management (MDM) software for all mobile devices and those used out of office. • Do not allow the use of jailbroken devices. • Establish and operate an ability to: o Track devices o Use appropriate file storage products o Remotely wipe corporate information on devices in the case of theft or inappropriate use o Implement encryption mechanisms to protect sensitive information o Implement proper mechanisms to disable portable computing devices o Proper data backup procedures for the portable computing devices o Limit or restrict usage of portable computing devices to authorized users with adequate security controls • Regularly review, update as needed and reissue/publish the policy document. Gain formal acknowledgement of such changes from all users.
Administrative	• Enforce MDM policies that include configuration of the device, encryption of removable storage cards (SD cards in mobiles etc.), passcode enforcement, detection of jailbroken device. • Determine out-of-date operating systems and notify users to update. • Remotely wipe entire devices or selectively wipe corporate data as requested.
End Users	Be aware that sometimes only data held in certain applications – such as email – can be wiped.

Table 47: Mobile Device Working – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	**Procedure description**
Management	Implement policy defining the applications that can be used for particular purposes. For example, the use of specialist applications for things such as medical picture taking, also support attachment of that picture to the clinical record.
Administrative	• Enforcement of MDM policies. • Examine the potential for the use of micro VPN technologies where possible to prevent resident data on devices. • Secure applications for access and synchronisation of files rather than email being used as workaround.
End Users	No additional requirements in this section

Table 48: Mobile Device Working – Enhanced Procedures

6.1.16. Domain 16: Electronic Bio-Medical Devices

a. Objective

(i) Identify and classify the EBMD belonging to the HealthCare Facilities.

(ii) Provide mandatory and recommended controls for securing EBMDs.

(iii) Ensure EBMD(s) are continuously maintained to an appropriate security baseline

(iv) Non-electronic biomedical devices are not scoped under this standard.

b. Policy requirements

A suitable high-level policy must consider and address at least:

(i) Responsibilities for managing the EBMD(s) in the HealthCare Facilities.

(ii) Classification of EBMDs (as per the classification scheme provided in appendix 6).

(iii) Storage, handling and secure disposal of EBMD(s).

c. Procedures

(i) Essential procedures

Responsibility	**Procedure Description**
Management	• Ensure the classification procedures in line with the classification principles laid down in Annexure A are approved and authorized for use suitable for HealthCare Facilities EBMD environment

Responsibility	Procedure Description
	- Procedures to request, update, store - Manufacturer Disclosure Statement for Medical Device Security – MDS2 shall be established. - The procurement process of EBMD in HealthCare Facilities shall ensure that manufacturers / Principle Vendors / Suppliers provide the following information related to the security of the EBMD before its deployment in HealthCare Facilities (s): ✓ The intended use of the device. ✓ Risk assessment report and controls put in place to protect the EBMD, including: o A specific list of all security risks that were considered in the design of the EBMD. o A statement about who conducted the risk assessment, and who approved it. o A statement about technical security testing that was conducted, by whom, and what the results were. o A specific list and justification for all security controls that were established for your device, and a justification for all controls from this standard that were omitted. o A traceability matrix that links the security controls to the risks that were considered. ✓ A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to continue to assure its safety and effectiveness. ✓ An indication whether the EBMD will be remotely accessed, and if so, which controls are in place to secure that access. ✓ A summary describing controls that are in place to assure that the EBMD software will maintain its integrity (e.g. remain free of malware) from the point of origin to the point at which that device leaves the control of the manufacturer. ✓ Device instructions for use and product specifications related to recommended security controls appropriate for the intended use environment (for example, anti-virus software or use of firewall).

Responsibility	Procedure Description
Administrative	- Adhere and develop associated asset labelling as per the laid down procedures. - Ensure proper labelling, filing and serialization of MDS2 w.r.t each or group of EBMD(s) used in HealthCare Facilities. - Ensure Risk Assessment reports from the procurement process are reviewed and available readily for reference.
End Users	No additional requirements in this section

Table 49: Electronic Bio-Medical Devices – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure description
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 50: Electronic Bio-Medical Devices – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure description
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 51: Electronic Bio-Medical Devices – Enhanced Procedures

6.1.17. Domain 17: Cloud Computing

a. Objective

(i) To ensure HealthCare Facilities have security controls applied by cloud service providers to their information.

(ii) These security controls have to be applicable, clearly specified and where appropriate, are built into contractual arrangements for that service.

(iii) To ensure that security controls in HealthCare facilities as a minimum, cover the following factors:

- Transmission.
- Storage.
- Processing of information.
- Data center infrastructure (such as physical access controls, third-party or sub providers credentials, building code compliance).
- Encryption and decryption of data (where, when, how).
- Recovery of client information and /or applications by the HealthCare Facilities.
- Access to client information by third parties.

(iv) To ensure HealthCare facilities have a clear understanding of the model adopted with its attendant risks, rights and obligations as specified in a cloud computing contract, forms an essential risk management tool to support the security of information.

b. Policy requirements

A cloud security policy must be formalized and identify with at least the areas below:

(i) The classification, sensitivity and security factors of information to be stored, processed or transiting the cloud service.

(ii) The availability of information.

(iii) The cloud organization incident management, jurisdictional and contractual arrangements.

(iv) The third-party provider (inter-) dependencies and capabilities.

c. Procedures

(i) Essential procedures

Responsibility	Procedure description
Management	***Cloud sourcing*** • HealthCare Facilities shall not use cloud services or infrastructure to store, process or share information that contains Health Information outside the legal jurisdiction or geographical boundaries of the United Arab Emirates, including for CSP's Backup or Disaster Recovery purposes. • Dubai government and semi government entities shall ensure mandatory compliance with DESC CSP security standards for all CSPs offering cloud services. ***Cloud security policy*** Establish or adopt and adapt the security aspects of an existing reputable cloud security policy that addresses the HealthCare Facilities's requirements for overall cloud management process and outlines roles and responsibilities of relevant stakeholders ***Risk assessment*** Perform a security risk and assurance assessment on any cloud computing initiative as part of the HealthCare Facilities's cloud security policy. ***Sovereignty*** • Ensure through a formal agreement that the CSP has no ownership rights on the stored data regardless of the format or storage medium. • Document the considerations, assessment and method of addressing any identified sovereignty issues or risks relating to information security. ***Governance*** Ensure the provider's service level agreement and usage terms are fit for purpose and in place in relation to information security. ***Confidentiality***

Responsibility	Procedure description
	Define and communicate required security controls to CSP for handling of data in accordance to the applicable laws & regulations ***Integrity*** Ensure through a formal agreement to address the security requirements for change management process. ***Availability*** • Proper cloud security controls are implemented by CSP, addressing HealthCare Facilities's requirements for periodic testing of continuity and disaster recovery plans. • Adequate measures and processes to support data portability in place whenever the HealthCare Facilities decides to move its data. ***Incident response/management*** Confirm effective incident management and response processes for information security are in place. (see also section 17 – Domain 10: Information Security Incident Management)
Administrative	• Ensure adequate cloud security controls are implemented by CSP as per architecture and deployment model approved by the entity. • Conduct periodic reviews or audits to verify CSPs' compliance with the applicable security policies and contractual requirements.
End Users	On an ongoing basis report on unusual operational security aspects that affect the ability of the user to operate in the stated policy areas.

Table 52: Cloud Computing – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure description
Management	***Cloud sourcing*** • Select a provider who complies with the information security policy by undertaking a formal request for proposal process. • Ensure that CSPs are certified as per the CSP security standard's certification process outlined by DESC. ***Sovereignty*** • Formally identify and assess CSPs storage/processing sites for information. This may include proposed back-up and replication sites/locations. • Review other legislation/regulation as well as the cloud computing health care provider's access request processing protocols. ***Governance*** Ensure the supplier service delivery assessment includes evidence around commercial integrity, resiliency, reliability and longevity as well as compliance to security practices. ***Confidentiality*** • Confirm the cloud computing organisation operates an appropriate (role based) identity access management system. • Confirm the cloud computing organisation protects HealthCare Facilities Health Information appropriately, such as the provision/enabling of approved encryption of data at rest and in transit. ***Integrity*** • Identify and assess the operating environment, employment procedures, and physical and systems security assertions made by the selected CSP. • Confirm agreed record destruction processes are in place. ***Availability*** Identify and assess service level agreement availability specifications. ***Incident response/management*** Identify and assess service level agreement incident specifications.
Administrative	On an ongoing basis, the system is to record and report significant variances in or changes to or within the operation of the policy areas.
End Users	No additional requirements in this section.

Table 53: Cloud Computing – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure Description
Management	• Ensure that the cloud service provider applies OS and Applications security hardening best practices. • Ensure that the cloud service provider applies periodic penetration testing and that a remediation program is defined, and it includes fixing the vulnerabilities based on priority. All vulnerabilities shall be prioritized and must be fixed and patched within SLAs.
Administrative	No additional requirements in this section.
End Users	No additional requirements in this section

Table 54: Cloud Computing – Enhanced Procedures

Contact Us

Still have questions?

For more information on NABIDH, please reach out through the following channels:

800 DHA (800 342)	info@dha.gov.ae	https://nabidh.ae

This document was last updated on **01 Sep 2020**

800342 (DHA) | dha.gov.ae | @dha_dubai | Dubai Health Authority | DHA