# INFO5301 Information Security Management

## Assignment 2

**Group 8 - CC05**

Andrea Aquino De Hoge -

Henriette Elise Onarh[redacted]

Mingrui Xiao -[redacted]

Ryo Nishig[redacted]

Zekai Gu[redacted]

[redacted]

# Table of Contents

**1. Audience** ..... **5**
**2. Purpose** ..... **5**
**3. Scope** ..... **5**
**4. General Principles** ..... **5**
**5. Information Security Controls** ..... **6**
5.1 Human Resources Security ..... 6
5.1.1 Human Resources Guidelines ..... 6
5.1.1.1 Audience ..... 6
5.1.1.2 Purpose ..... 6
5.1.1.3 Scope ..... 6
5.1.2 Information Security Control Guidelines ..... 7
5.1.2.1 Pre-Employment Controls ..... 7
5.1.2.2 During Employment ..... 7
5.1.2.3 Termination or Change of Employment ..... 7
5.1.2.4 Compliance and Legal Obligations ..... 7
**5.2 Asset Management** ..... **7**
5.2.1 Inventory of Assets ..... 7
5.2.2 Information and Data Classification: Manual ..... 8
5.2.2.1 Data Classification and Handling Manual ..... 8
5.2.2.1.1 Audience ..... 8
5.2.2.1.2 Purpose ..... 8
5.2.2.1.3 Scope ..... 8
5.2.2.1.4 Executive Summary ..... 8
5.2.2.1.4 Data Classification ..... 9
5.2.3 Information Handling ..... 10
5.3 Access Control ..... 11
5.3.1 Access Control Manual ..... 11
5.3.1.1 Audience ..... 11
5.3.1.2 Purpose ..... 11
5.3.1.3 Scope ..... 11
5.3.1.4 Executive Summary ..... 11
5.3.1.5 Principles ..... 12
5.3.1.6 Procedures ..... 12
5.3.1.7 Access Control ..... 12
5.4 Physical and Environmental Security Manual ..... 12
5.4.1 Audience ..... 13
5.4.2 Purpose ..... 13
5.4.3 Scope ..... 13
5.4.4 Requirement ..... 13
5.4.5 Secure Areas (Best Practice, 2020; Edwards, 2023) ..... 13
5.4.5.1 Physical Security Perimeter ..... 13
5.4.5.2 Physical Entry Controls ..... 13
5.4.5.3 Securing Offices, Rooms, and Facilities ..... 13
5.4.5.4 Protecting Against External & Environmental Threats ..... 13
5.4.5.5 Working in Secure Areas ..... 14

5.4.5.6 Delivery & Loading Areas....14
5.4.6 Equipment (Best Practice, 2020; Edwards, 2023).... 14
5.4.6.1 Supporting Utilities.... 14
5.4.6.2 Cabling Security.... 14
5.4.6.3 Equipment Maintenance.... 14
5.4.6.4 Removal of Assets.... 14
5.4.6.5 Security of Equipment and Assets Off-Premises.... 14
5.4.6.6 Secure Disposal or Re-Use of Equipment.... 14
5.4.6.7 Unattended User Equipment....15
5.4.6.8 Clear Desk and Clear Screen Policy....15
5.5 Operations Management.... 15
5.5.1 Information Security Operations Management Manual....15
5.5.1.1 Audience.... 15
5.5.1.2 Purpose....15
5.5.1.3 Scope....15
5.5.1.4 Operational Procedures.... 15
5.5.1.5 Responsibilities.... 15
5.5.1.5.1 Health Information Managers....15
5.5.1.5.2 Health Information Technicians.... 16
5.5.1.5.3 Clinical Staff (Doctors/Nurses).... 16
5.5.1.5.4 Facilities Management Staff....16
5.5.1.5.5 Change Management....16
5.5.1.5.6 Risk and Vulnerability Management....17
5.5.1.6 Operations Security....17
5.5.1.7 Controls Against Malicious Code.... 17
5.5.1.8 Backup.... 18
5.5.1.9 Log Management.... 18
5.5.1.10 Vulnerability Management & Information Security Patch Management Manual..... 18
5.5.1.10.1 Audience.... 18
5.5.1.10.2 Purpose....18
5.5.1.10.3 Scope.... 19
5.5.1.10.4 Patch Management Process.... 19
5.5.1.10.5 Identify Vulnerabilities and Their Patches.... 19
**5.6. Network Communications Security.... 20**
5.6.1. Audience....20
5.6.2 Introduction and Purpose....20
5.6.3. Network Policy Scope....20
5.6.4 Network Infrastructure Overview....21
5.6.4.1 Network Segmentation....21
5.6.4.2 Network Design Diagram.... 21
5.6.4.3 Encryption of In-Transit Data....21
5.6.5 Network Monitoring and Logging.... 22
5.6.5.1 Access Control List (ACL)....22
5.6.5.2 Monitoring Access and Network Devices Access Procedures....22
5.6.6 Firewall....22
5.6.7 Intrusion Detection/Prevention Systems (IDS/IPS) (Infosec, n.d.)....23

5.6.8 Security Email System..... 23
5.6.9 Audit and Reviews of Network Control and Measurements..... 23
**5.7 Information Security Incident Management..... 23**
5.7.1 Security Incidents Classifications..... 24
5.7.2 Reporting an Incident..... 24
5.7.3 Incident Response and Assessment..... 24
5.7.4 Incident Containment and Mitigation..... 24
5.7.5 Incident Investigation and Analysis..... 24
5.7.6 Incident Resolution and Recovery..... 24
5.7.7 Communication and Reporting Incidents..... 25
5.7.8 Acknowledgement..... 25
5.7.9 Culture of Security..... 25
**6 Roles and Responsibilities..... 25**
6.1 Chief Digital & Information Officer..... 25
6.2 Information Owner..... 25
6.3 System Owner..... 25
6.4 System Administrator..... 26
6.5 Information Security Team..... 26
**7 References..... 27**
**8 Appendix (Justification of Exceeded Pages and Work Distribution)..... 31**

# Healthcare Organisation - A Hospital

## 1. Audience

This Information Security Policy applies to all employees, contractors, and related third parties who have access to the Hospital's information systems and data. This includes all administrative staff, medical staff, part-time and temporary workers, consultants, and outsourced service providers (Guard24, 2023). The policy also applies to any external stakeholders who interact with our systems, such as suppliers and insurance companies. In some cases, patients also need to obey this policy.

## 2. Purpose

The purpose of this Information Security Policy according to ISO27001 (G, 2023) is to establish and promote the secure management of our hospital's data and information systems. The policy is designed to protect our assets from a variety of threats, internal or external, intentional or accidental, to ensure the confidentiality, integrity, and availability of patient and business data (Kostadinov, 2020).

## 3. Scope

The scope of this policy includes all systems, data, networks, and software applications operated by or on behalf of the main office of the hospital, as well as all forms of information, including electronic, printed, and other physical forms handled at the main office. It covers all locations where hospital information can be accessed, including remotely from home or in transit (Kostadinov, 2020).

## 4. General Principles

General Principles will mainly go into 5 principles that are Confidentiality, Integrity, Availability, Authentication, and Non-repudiation (6clicks, n.d.).

(1) Confidentiality: Ensure that patient information and other sensitive data are accessible only to authorised personnel. Confidentiality measures must prevent unauthorised access, disclosure, or interception of data (Colling & York, 2009).
(2) Integrity: Data must be accurate, complete, and reliable. Implement controls to protect against unauthorised data modification or deletion, and ensure that any changes to information are traceable and auditable.
(3) Availability: Ensure that authorised users have continuous access to information systems and data when needed (Murphy, 2015). This includes implementing measures to protect against disruptions like hardware failures, software issues, or cyber attacks.
(4) Authentication: Authentication is a fundamental principle of information security that involves verifying the identity of a user, system, or entity before granting access to sensitive data and systems.
(5) User Responsibility: Define responsibilities for information security for all staff members. Regular training and awareness programs should be conducted to keep staff informed about their roles in maintaining information security (Woodley, n.d.).
(6) User Comply: The hospital needs to comply with HIPAA or other data protection laws. All employees are required to comply with all organisational security policies and processes.

(7) Risk-Based Approach: Risk assessment is vital in the hospital setting. Including identifying and evaluating potential threats such as cyber threats, human errors, or system failures. Based on the risk levels to allocate resources.

# 5. Information Security Controls

## 5.1 Human Resources Security

### 5.1.1 Human Resources Guidelines

Human Resources (HR) plays a crucial role in any organisation, not only ordinary companies but also in special environments, especially hospitals. In a hospital, HR is important in a wide range of functions that can prove the overall effectiveness, efficiency, and culture of the hospital. Human Resources Security is the most important area of information security. All cyber security issues occur due to people and HR security leads directly to this scope, HR can control the quality of employees by the rules and proper auditing to make sure the security of the hospital. HR security starts from the moment a potential employee starts to work in the hospital and continues until after they leave the hospital (Lindquist, 2023). This includes various policies and procedures designed to reduce the risk of theft, fraud, or misuse of facilities and other threats.

#### 5.1.1.1 Audience

The audience for the Human Resources Security policy (GNYHA, n.d.).

(1) Human Resources (HR) Staff: Who are directly involved in hiring, managing, and off-boarding employees.
(2) Hospital Management: Including senior executives and department heads who need to understand and enforce the policy.
(3) All Hospital Employees: Including permanent, temporary, and contract staff, they need to be aware of their roles and responsibilities concerning information security.
(4) IT and Security Teams: Collaborate with HR to implement and monitor security controls related to user access and data management.
(5) External Partners and Contractors: These need to comply with the hospital's security policies when they have access to the hospital's systems and data (GNYHA, n.d.).

#### 5.1.1.2 Purpose

The purpose of the Human Resources Security policy will be to protect sensitive information such as patient data, to make sure that it must be accessed only by authorised personnel and protected against unauthorised access, use, disclosure, alteration, or destruction. HR needs to raise awareness and understanding of information security risks and best practices among all hospital staff. This will be the most efficient way to protect the hospital. And need to comply with legal and regulatory requirements related to data protection and privacy, such as HIPAA (United States Department Of Labor, 2004) or other regulations. These all can minimise the risk, addressing human factors in security breaches, and ensuring the staff are appropriately vetted, trained, and monitored throughout their tenure.

#### 5.1.1.3 Scope

The scope manual of the Human Resources Security policy covers all employment lifecycles from pre-employment to post-termination ones. All forms of data, security education, and awareness (Hospital

HR, 2023.). Also covers access control and physical and logical access that will be introduced in the below sections.

### 5.1.2 Information Security Control Guidelines

#### 5.1.2.1 Pre-Employment Controls

Conduct a full background check, including employment history, previous company assessment, criminal record, educational background, references, and medical examination reports. This is especially important for positions that concern sensitive data. When deciding to employ them, they need to provide an optimised security awareness and training before starting work. Training includes the hospital's information security policy, data protection requirements, and responsibilities. At last need a contractual agreement that contains clauses that clearly define the policy about security responsibilities and legal/regulatory requirements (Croskey & Terry, 2020).

#### 5.1.2.2 During Employment

Employment needs ongoing training and awareness, regular training based on security policies, data protection practices, and new emerging security threats treatments. This may even need to be customised to specific roles. Implement controls to manage the addition, modification, and deletion of access rights by HR processes and review access rights regularly. Auditing, reviewing, and monitoring the employee security performance, then point to any violations or weaknesses and take appropriate action to prevent or control them. If the employee gets promotions, transfers, or demotions needs to be re-evaluated access rights (Australian Medical Association, 2018).

#### 5.1.2.3 Termination or Change of Employment

When an employee leaves the hospital or changes position, the hospital needs to establish a formal separation process, it includes returning all asserts, removal of access rights, and debriefing on ongoing confidentiality requirements. There are several restrictions for termination, such as continuing to protect the hospital's information even after the employment relationship ends. Before formal termination, arrange an exit interview to understand the reasons for termination and collect feedback on security policies (Australian Medical Association, 2018).

#### 5.1.2.4 Compliance and Legal Obligations

HR is the duty of legal training about aspects of handling personal and sensitive information, and maintaining security compliance records such as training records, background checks, and security incidents (NSW Health, 2020).

## 5.2 Asset Management

### 5.2.1 Inventory of Assets

Managing assets, especially in a healthcare setting like a hospital, is crucial for ensuring financial sustainability, patient care and efficient operations (Gavrikova et al., 2020). The inventory of assets contains both physical and intangible objects, and they need to be managed carefully to ensure that sensitive data remains protected from unauthorised access.

The assets should be recorded in a database that contains a detailed inventory of both physical and intangible assets. It is essential that all assets are tracked regularly and contain information regarding item

descriptions, cost, locations, acquisition dates and other relevant data (Paloalto, n.d.). This could also help with maximising utilisation of assets, which could further result in minimisation of waste and unnecessary expenses (Linuhung & Mediawati, 2023). It is especially important to keep track of expiration dates of medical supplies and pharmaceuticals, as this could have severe consequences if used improperly. There are also regulations and standards, such as Therapeutic Goods Administration, that the hospital will need to comply with to ensure proper usage of medical equipment supplies (Ghosh et al., 2006). This includes having to register all medical devices with TGA, perform regular checks to ensure high quality of the equipment and notify of faulty and fraudulent devices (Grove, 2019).

Furthermore, the inventory should also keep track of the medical equipments' current working condition such that repairs can be scheduled if needed. Preventative maintenance protocols should be established as well to reduce the risk of broken equipment, and this information should be included in the asset records (Li et al., 2022). Software systems for asset management, such as Enterprise Asset Management, should be utilised to make the management easier and more organised (Keller, 2014). It should also be possible for medical professionals at the hospital to search up items and update relevant information. Note that access control needs to be implemented as well, however this will be further explained in the sections below.

## 5.2.2 Information and Data Classification: Manual

The following manual's structure is influenced by University of Newcastle's guidelines on information security data classification and handling (University of Newcastle, 2017). It provides in-depth instructions on how the hospital handles data and uses data classification to ensure confidentiality. It also contains a table outlining the impact and severity of sensitive data being disclosed to unauthorised personnel according to the data's classification level.

### 5.2.2.1 Data Classification and Handling Manual

#### 5.2.2.1.1 Audience

(1) This manual is applicable to all staff members, contractors, third-parties and other individuals who have access to or handle data within the hospital.

#### 5.2.2.1.2 Purpose

(2) The purpose of this manual is to establish guidelines for data classification within the hospital to ensure that there is consistency in the labelling and handling of data.
(3) Establishing the classification levels is the Information Owner's responsibility. The classification is based on the data's sensitivity, criticality and legal requirements (Katarahweire et al., 2020).
(4) The guidelines apply to all assets handled by the hospital, irrespective of whether they are in a physical or intangible form

#### 5.2.2.1.3 Scope

(5) The scope of this manual includes the audience listed above, and covers guidelines for data classification to ensure consistency in data handling across all assets handled by the healthcare organisation. It also establishes classification levels based on data sensitivity and legal requirements

#### 5.2.2.1.4 Executive Summary

(6) The hospital collects, stores, processes and transmits information that is needed for its operations. It is of utmost importance to safeguard this information against unauthorised access and misuse,

while also ensuring accessibility for authorised healthcare personnel that need the data to perform their job duties

(7) This manual establishes guidelines and instructions on the hospital's data classifications, and the protocols that healthcare personnel need to follow in order to safeguard information

(8) The protocols for data classification outlined in this manual ensure that the hospital complies with privacy regulations and health legislations such as the Privacy Act 1988, General Data Protection Regulation and Health Records and Information Privacy Act 2002 No 71 (Federal Register of Legislation, 2023; GDPR, n.d.; NSW Legislation, 2023). The system must also follow the requirements outlined by ISO 27001, the international standard for information security (Kosutic, n.d.).

#### 5.2.2.1.4 Data Classification

(9) The hospital uses four levels of confidentiality as follows:
   (a) Public: low sensitivity and does not require disclosure
   (b) Protected: employees at the hospital can access this information
   (c) Restricted: confidential data that will only be accessed by a limited number of healthcare personnel
   (d) Highly restricted: highest level of sensitivity, only accessible by authorised personnel that needs the information to perform job duties

(10) The data classification levels follow NSW and Commonwealth's security classification system with the exception of the "TOP SECRET" level (Data NSW, 2023). The reasoning behind this is that top secret labels should only be used when disclosure of data could cause severe damage to the national interest, which is irrelevant to healthcare organisations such as hospitals.

(11) The Information Owner should consider the impact and severity of data being disclosed to unauthorised personnel, stolen or lost. The table provided below should be used when classifying data into the appropriate classification level.

**Figure 1**

*Severity of Implications in Data Classification Levels*

| | **Severity** | | | |
|---|---|---|---|---|
| **Suggested data classification level** | **Public** | **Protected** | **Restricted** | **Highly restricted** |
| **Impact** | **Insignificant** | **Moderate** | **Major** | **Severe** |
| Legal complications | No penalty or legal impact | Minor legal penalties or reviews required by legislator | Potential for legal action such as sanctions and penalties by regulatory authorities | Severe legal complications that could significantly impact the hospital, both financially and legally |
| Operational performance | No significant impact on the hospital's operations | Minor impact and inconvenience | Performance is disrupted | Potential for a significant disruption |
| Healthcare personnel | Employees unaffected | Minor impact on employees' welfare and safety | Significant impact on employees, risk of external authorities getting involved | Severe impact on employees, risk of permanent damage |

| | | | | |
|---|---|---|---|---|
| Financial | Insignificant costs | Costs of up to 5% of hospital's budget (University of Newcastle, 2017) | Costs of up to 10% of hospital's budget (University of Newcastle, 2017) | Costs more than 10% of hospital's budget (University of Newcastle, 2017) |
| Reputation risk | No damage to reputation | May cause concern for patients, risk of criticism | High impact on hospital's reputation, significant loss in trust by patients | Could cause permanent damage on hospital's reputation which may impact its existence |
| Examples | Publicly available research publications, hospital events and outreach programs, non-sensitive data regarding hospital facilities | Internal policies and manuals for hospital staff, contact information for employees, communication intended for staff | Patient data that do not contain particularly sensitive information such as ethnicity and gender. Medical imaging only accessible to radiologists | Health status and patient records containing particularly sensitive information such as Protected Health Information (PHI) and Personally Identifiable Information (PII), e.g. passport number and driver's licence |

*Note*. Table created by the group.

### 5.2.3 Information Handling

When handling the hospital information, there are a number of factors that need to be taken into consideration in order to ensure compliance with regulatory authorities:

(1) Data collection
    (a) Upon gathering data, established procedures should be followed to ensure accuracy and that the acquisition process follows legal requirements such as informing the patient of the data collection and obtain consent
(2) Data storage
    (a) As briefly mentioned in previous sections, data should be stored securely in the inventory to prevent against unauthorised access
    (b) Encryption should be used on particularly sensitive data
(3) Data transmission
    (a) Established mechanisms including encryption and authentication should be used when transmitting data between hospital departments, healthcare partners and other third-parties
(4) Data processing
    (a) Processing of healthcare data should be communicated to the patient such that there is transparency
    (b) De-identification techniques and differential privacy should be considered if the processed data is particularly sensitive
(5) Data removal
    (a) According to regulatory authorities such as GDPR, data should not be retained for longer than necessary and should be removed when the data is no longer needed for processing (GDPR, n.d.)
(6) Data updating
    (a) It is of utmost importance to ensure that data is regularly updated in order to ensure accuracy

(7) Data auditing
    (a) In order to ensure that only authorised personnel accesses data, there should be logs and records which ensure continuous monitoring and auditing

## 5.3 Access Control

As mentioned in the previous part about data classification, implementing proper access control is essential in order to prevent unauthorised access of sensitive data. The manual below serves as a comprehensive guide for all healthcare personnel at the hospital who have access to or handle data within the premises.

### 5.3.1 Access Control Manual

#### 5.3.1.1 Audience

(1) This manual is applicable to all staff members, contractors, third-parties and other individuals who have access to or handle data within the hospital

#### 5.3.1.2 Purpose

(2) The purpose of this manual is to outline the policies and procedures that should be followed when providing access to hospital assets and resources. The aim is to maintain confidentiality, integrity and availability while ensuring regulatory compliance

#### 5.3.1.3 Scope

(3) The scope of this manual includes the audience listed above, and covers the implementation of role-based access control and access control lists within the hospital, along with a hybrid approach between the Biba and Bell-LaPadula models for ensuring both confidentiality and integrity of sensitive data.

#### 5.3.1.4 Executive Summary

(4) The hospital uses a combination of role-based access control and access control lists to restrict access to sensitive data and systems based on job responsibilities. Both confidentiality, integrity and availability is considered, and the access control roles are heavily influenced and correspond with the data classification levels outlined in the “Data Classification and Handling” manual
(5) A hybrid approach between the Biba model and Bell-LaPadula model will be applied to ensure that not only confidentiality is ensured, but also integrity. The approach used depends on each specific case and their sensitivity level
    (a) Biba is applied when maintaining integrity is the priority (Sandhu, 1993)
        (i) For example, a medical professional at the protected level cannot write to sensitive medical data at restricted and highly restricted levels, as write-access is limited to specialised staff
    (b) Bell-LaPadula is applied when confidentiality is prioritised (Sandhu, 1993)
        (i) For example, a nurse within the restricted level may read patient records within their assigned ward, however they cannot read particularly sensitive information at the highly restricted level.
    (c) Each user can typically access all resources at their own level, however there are circumstances where access control rules can reject access

(i) For example, a medical professional at the highly restricted level may be able to access patient records at this level, however they cannot access highly restricted financial records as this is beyond their job duties

(6) Regular reviews of employees' roles will be conducted to ensure that they are accurate and up-to-date

#### 5.3.1.5 Principles

(7) Principles of least privilege: only healthcare personnel that need the specific data for their job responsibilities should be granted access (Plachkinova & Knapp, 2023)

(8) Need-to-know principle: information should be restricted based on roles and responsibilities (Liqing & Hai, 2021)

#### 5.3.1.6 Procedures

(9) User authentication should be used to verify the user's identity before granting access. Multi-factor authentication is preferred

(10) User authorisation should be used to ensure that users are allowed to perform tasks

(11) Specialised access control procedures should be used when third-party vendors need to access data temporarily. This includes strict oversight and monitoring.

#### 5.3.1.7 Access Control

(12) The following table outlines how access control is used in correspondence to the data classification levels outlined in the "Data Classification and Handling" manual. Its format and structure is influenced by the University of Newcastle's guidelines on information security data classification and handling (University of Newcastle, 2017).

**Figure 2**

*Access Control Within the Hospital*

| Access control | Public | Protected | Restricted | Highly restricted |
|---|---|---|---|---|
| No restrictions | X | | | |
| Only authorised healthcare personnel can access data | | X | X | X |
| Recommended to use multi-factor authentication | | X | X | |
| Required to use multi-factor authentication | | | | X |

*Note.* Table created by the group.

## 5.4 Physical and Environmental Security Manual

Physical and environmental controls assure protection of data and information, hardware, and human resource assets, including inappropriate physical access, theft, vandalism, accidental, intentional, and natural disasters. (The Institute of Internal Auditors, n.d.)

### 5.4.1 Audience

This manual is for all staff members, visitors, third-parties and other individuals who have physical access to the hospital

### 5.4.2 Purpose

The purpose of the document is to establish comprehensive physical and environmental security policies that protect the assets and information resources from unauthorised access, theft, damage, and other security threats.

### 5.4.3 Scope

The scope of physical and environmental security is to secure safeguards for the organisation’s physical and information assets: Division of Secure Areas, Equipment Security, Environmental Protection. (NSW Ministry of Health, 2022)

### 5.4.4 Requirement

Physical and environmental security has two types of requirements; Secure areas and secure equipment and maintenance. (Maya, 2023) The application to the medical institution is shown here.

### 5.4.5 Secure Areas (Best Practice, 2020; Edwards, 2023)

#### 5.4.5.1 Physical Security Perimeter

Defines the boundaries around the hospital's secure areas, including fences, walls, and controlled access points. (Maya, 2023; Taylor, 2023).The hospital is surrounded by tall fences with barbed wire on top, motorised gates monitored by security personnel via intercoms, and 24/7 video surveillance managed from a central security room.

#### 5.4.5.2 Physical Entry Controls

Controls who enters the hospital using secure technologies.(Maya, 2023; Taylor, 2023). Entry into the hospital is regulated with fingerprint scanners and a reception desk where visitors and staff must register and receive permission. All staff access, including restricted areas, requires both authentication with ID cards and fingerprints.

#### 5.4.5.3 Securing Offices, Rooms, and Facilities

Protects areas with valuable assets using strong security measures. (Maya, 2023; Taylor, 2023). Sensitive areas such as office spaces and patient records rooms are secured with fingerprint access controls. All sensitive documents are stored in locked cabinets, and digital systems are secured with robust encryption and continuous camera surveillance.

#### 5.4.5.4 Protecting Against External & Environmental Threats

Protect against natural and environmental risks.(Maya, 2023; Taylor, 2023). The hospital employs advanced fire suppression systems and flood defences including elevated barriers and sump pumps. Places where important data is stored have special fire alarms and chemicals sensors to detect dangerous substances.

#### 5.4.5.5 Working in Secure Areas

Ensures rules and security measures are followed in sensitive areas. (Maya, 2023; Taylor, 2023). Staff working in high-security zones must complete specialised security training and receive certifications. Mobile phones and recording devices are prohibited to secure confidentiality. They can't bring cell phones or cameras, and they always work in pairs for better security.

#### 5.4.5.6 Delivery & Loading Areas

Manages and secure areas where deliveries and shipments are handled. (Maya, 2023; Taylor, 2023). Delivery and loading zones are tightly controlled with security cameras and personnel. All delivery staff must undergo a check-in process at a dedicated security checkpoint, show identification, and have their vehicles inspected. Incoming packages undergo thorough security screenings before acceptance.

### 5.4.6 Equipment (Best Practice, 2020; Edwards, 2023)

#### 5.4.6.1 Supporting Utilities

Ensures systems that provide essential power and cooling are reliable and protected. (Maya, 2023; Taylor, 2023). All critical areas like operating rooms have reliable backup power that's regularly tested to function during outages.

#### 5.4.6.2 Cabling Security

Protects cables from damage and unauthorised access by organising and securing them appropriately. (Maya, 2023; Taylor, 2023). Network and power cables are routed through protective conduits and checked regularly by facility management to prevent damage and unauthorised access.

#### 5.4.6.3 Equipment Maintenance

Regularly maintains equipment to ensure it is functional and secure. (Maya, 2023; Taylor, 2023). Medical and IT equipment maintenance is performed quarterly by certified technicians, with all activities logged and reviewed by the IT department.

#### 5.4.6.4 Removal of Assets

Control the removal of assets from premises to prevent unauthorised asset transfer. (Maya, 2023; Taylor, 2023). Removing equipment from the hospital requires a department head's approval, a completed form, and tracking via inventory systems to prevent unauthorised transfers.

#### 5.4.6.5 Security of Equipment and Assets Off-Premises

Protect information and assets located or used outside the hospital premises. (Maya, 2023; Taylor, 2023). Mobile devices and laptops used off-site are secured with passwords, encryption, and GPS tracking to mitigate loss or theft.

#### 5.4.6.6 Secure Disposal or Re-Use of Equipment

Safely dispose of or reuse equipment to prevent unauthorised access to stored information. (Maya, 2023; Taylor, 2023). Decommissioned equipment is wiped according to security standards, physically destroyed or degaussed, and refurbished under strict conditions if reused.

#### 5.4.6.7 Unattended User Equipment

Secures unattended equipment against unauthorised access or damage. (Maya, 2023; Taylor, 2023). Unattended equipment must be password-locked and stored in locked cabinets, with random security checks for compliance.

#### 5.4.6.8 Clear Desk and Clear Screen Policy

Minimise the risk of unauthorised access to information when desks and screens are unattended. (Maya, 2023; Taylor, 2023). Staff must clear all sensitive documents and activate screensavers at shift end, with regular audits to ensure policy adherence.

## 5.5 Operations Management

### 5.5.1 Information Security Operations Management Manual

#### 5.5.1.1 Audience

The audiences for information security operations management policies within healthcare organisation are:

1. The healthcare organisation's information systems which information security operations operate on, especially which handle Electronic Patient Health Information (ePHI).
2. Anyone who operates (manages, interacts with, or is affected by the organisation's information systems) or influenced by information security operations (e.g. executives, healthcare professionals, IT staff).

#### 5.5.1.2 Purpose

The purpose of the information security operations management policies is to secure its information assets through ensuring the information confidentiality, integrity, and availability, as well as correct and secure operations of information systems, while following organisational policies, state laws, and regulatory compliance.

#### 5.5.1.3 Scope

The scope of information security operations management policies is all the staff and third-party services providers.

#### 5.5.1.4 Operational Procedures

The overall operational procedures for maintaining information security is:
Authentication -> Give access right -> Revoke access right (for classified information) -> Update log

#### 5.5.1.5 Responsibilities

##### 5.5.1.5.1 Health Information Managers

Oversee all activities related to the development, implementation, maintenance, and adherence to the organisation’s policies and procedures covering the privacy and security of patient health information. Conduct regular risk assessments and audits to identify potential vulnerabilities, evaluate the effectiveness

of security measures, and ensure compliance with health information privacy, security standards and state laws.

#### 5.5.1.5.2 Health Information Technicians

Organise, manage, and monitor health information data, ensuring it maintains its quality, accuracy, accessibility, and security in both paper files and electronic systems. Implement and maintain technical safeguards like encryption, firewalls, multi-factor authentication (Bhattasali & Saeed, 2014), and intrusion detection systems to protect electronic health information. Implement access controls to restrict access to ePHI to only those individuals who require it for their job functions. Regularly update and patch systems.

#### 5.5.1.5.3 Clinical Staff (Doctors/Nurses)

Collecting comprehensive patient data upon admission and throughout the care process, including medical history, diagnoses, treatment plans, and outcomes. Ensuring all healthcare interactions and interventions are accurately documented in the patient's health record in a timely manner. Report any issues regarding information security.

#### 5.5.1.5.4 Facilities Management Staff

Oversee and conduct maintenance and repairs of information equipment, implement a preventive maintenance schedule for office information equipment to ensure they are functioning correctly and minimising the risk of damaging or losing information. Implement safety protocols to mitigate potential information lost due to fire, flood, and so on.

All staff should maintain patient confidentiality and adhere to privacy practices, organise/participate in security awareness programs, and adhere to facility safety policies and procedures. All staff should be responsible for:

1. Ensure confidentiality, integrity, and availability of patient information, maintain accurate and complete patient health records
2. Maintain medical and office equipment, ensure cleanliness and safety of the facility
3. Protect electronic health information
4. Follow information security policies
5. Regular security assessments and training

#### 5.5.1.5.5 Change Management

Procedures to be taken while conducting organisational change which involves information security operations.

- **Phase 1: identify the change**
    - The IT department (potentially other departments as well) identify the need for change, the objectives of change. Before reporting to the higher level, they must develop a detailed explanation and plan for change with full assessment of possible organisational impact (e.g. financial).
- **Phase 2: report the need for change**
    - Report and communicate the change to higher level managers or executives, including why the change should be considered, the benefits it will bring, and how it will be implemented. If approved, continue to Phase 3, otherwise renounce the idea, or modify the change plan and propose again.
- **Phase 3: Implement the change while providing organisational awareness programs**

    - With approval, implement the change, while ensuring that all staff members affected by the change receive the necessary training and support. Thorough testing must be conducted before the actual launch.
- **Phase 4: Keep consolidating and refining change**
    - Monitor and evaluate the change by collecting user feedback, analysing performance data, and conducting review meetings, then adjust accordingly. Ensure that the change is fully integrated into the organisation's standard operating procedures by appealing the higher level to update organisational policies and procedures.

#### 5.5.1.5.6 Risk and Vulnerability Management

1. First, identify the assets involved in the information security operations. Then, we identify risks and vulnerabilities on those assets by regularly using automated tools to scan information systems and applications for vulnerabilities that could be exploited by cyber threats, inner threats, and natural disasters. We must stay informed about the latest cyber threats and vulnerabilities affecting the healthcare sector through threat intelligence feeds and information sharing with other healthcare organisations and agencies.
2. Assess and prioritise risks & vulnerabilities by conducting a thorough analysis to evaluate the potential impact and likelihood of identified risks or vulnerabilities being exploited. Use the former analysis results to label (CVSS) risks and vulnerabilities with different security levels (Nikoloudakis, et al., 2019), then prioritise remediation efforts on those with the highest severity and probability of exploitation.
3. Apply security controls to mitigate the risks and vulnerabilities by implementing appropriate technical, administrative, and physical security controls (e.g. encryption, intrusion detection systems, and revised security policies). In the meanwhile, continuously monitor the performance of such controls to detect inefficiencies to optimise, while conducting necessary employee awareness training.

The previously identified risks/vulnerabilities within the healthcare organisation include ransomware attacks, data breaches, lost or stolen devices, and phishing scams, which were mitigated via antivirus software, encryption on both data and device, and conduction of awareness training respectively.

### 5.5.1.6 Operations Security

Refer to a. Operational procedures and responsibilities

### 5.5.1.7 Controls Against Malicious Code

To control against malicious code, we have:

1. Deployed antivirus software to detect malware across all endpoints, servers, and networks within the healthcare organisation and ensured that they are updated frequently to protect against the latest threats from both within and without the organisation.
2. Deployed firewalls to monitor and control incoming and outgoing network traffic based on predetermined security policies; deployed intrusion detection systems to detect and prevent attacks by monitoring network and system activities for malicious actions or policy violations.
3. Deployed email filtering solutions to scan and block incoming emails for malicious attachments and links to prevent phishing attacks. We only allow approved software to run on network devices.

#### 5.5.1.8 Backup

We prioritise data based on their critical level (top secret, secret, confidential, public) to our healthcare organisation. The prioritised information like patient information, health records, and financial records have precedence.

If we are currently running on a sufficient resource, we do the backup both by ourselves and by cloud providers at the same time. Within our organisation, we follow the automated 3-2-1 backup solution (Magnusson, 2018), meaning keep at least three copies of information, store two backup copies on different storage media, and keep one of them offsite for disaster recovery. We must ensure that backups are consistently performed and up to date, and the possibility of staff mistakes is minimised by updating and inspecting the backups routinely. We also use reliable cloud services (Amazon HIPAA, which has been proved efficient and trustworthy while handling health information), while considering factors such as compatibility with our existing systems, ease of use, scalability, support for secure and encrypted backups, and compliance with healthcare information and regulations. We ensure all backup data is encrypted both in transit and at rest, as well as implement strict access controls and authentication mechanisms to protect sensitive patient information from unauthorised access. We have also deployed mechanisms to restore the data, like adopting RAID 6 model on disk backups.

If currently running on insufficient resources, the detailed temporary backup plan will be decided by C-suite.

#### 5.5.1.9 Log Management

We store the logs locally to reduce overhead. We have 3 servers within the healthcare organisation to manage the logs, each of which is maintained by our IT department. We must ensure that logs are collected from all relevant sources correctly, including electronic health record systems, network devices, security appliances, and servers. We use the logs to mainly perform the security analysis, by formally auditing the log once a week to check if we have the abnormal entries in our log. We also implement real-time monitoring of logs to identify and alert on suspicious activities and potential security incidents promptly. We deployed automated tools designed by our IT technicians for log analysis to efficiently sift through large volumes of log data, identify anomalies, and flag events of interest for further investigation. We use both physical (gates, guards) and software level controls (encryption) to ensure that logs are protected against unauthorised access and tampering. We must be mindful of privacy concerns when logging information, we must collect and retain the log while following the organisational policies. By default, logs stored in the servers will be saved for 50 years, after this, the logs will be moved to physical mediums (e.g. disk) which are maintained by the organisation’s database department.

#### 5.5.1.10 Vulnerability Management & Information Security Patch Management Manual

##### 5.5.1.10.1 Audience

Refer to a.Audience

##### 5.5.1.10.2 Purpose

Protecting sensitive patient data and ensuring critical services can be provided constantly. By identifying, evaluating, and mitigating security vulnerabilities in software and systems, and then promptly applying patches to fix these vulnerabilities, many security breaches can be prevented, so that the risks of

disclosed patient privacy, compliance violations, and operational disruptions can be minimised, thus helps maintain the CIA triad of health data.

#### 5.5.1.10.3 Scope

1. IT Security Team (directly involved in identifying, assessing, mitigating vulnerabilities and implementing patches)
2. IT Administrators (oversee operations of IT security Team)
3. Healthcare organisation's executives & CISO office (provide leadership and strategic direction for the IT department, including resource allocation, compliance, and management)

#### 5.5.1.10.4 Patch Management Process

The process is defined as follows:

1. IT management and the security team work together to regularly monitor the organisation's IT assets to identify vulnerabilities and their patches. The team should use IBM QRadar, since it has been proved to be capable of providing the healthcare organisation with a tool that has comprehensive visibility, advanced analytics, good scalability, workflow automation and compliance Support. Once vulnerabilities are found, the tech team may consult software vendors and security advisories for information about patches that can be installed to mitigate such vulnerabilities (Kandasamy et al., 2022). Or they can proactively install newly published patches to prevent vulnerabilities from being exploited (after thorough local testing).
2. IT management and the security team work together to draft a patch plan (e.g. which asset can be influenced by the vulnerability and why it needs to be patched, what are the benefits) and report it to the executives (CISO) to seek approval.
3. The executives (CISO) should evaluate the patch plan based on the organisation’s interest (e.g. if this helps create value for the organisation). With clearance, IT team test patches in a controlled environment to assess potential impacts on system stability and application compatibility, while documenting any issues encountered during testing to adjust the deployment plan as necessary.
4. The IT team deploy the patches (during off-peak hours if possible) according to priority (CVSS scoring system should be used here), starting with critical systems and vulnerabilities.
5. The IT team monitors the performance to verify that patches have been successfully applied and that systems are functioning as expected. Keep monitoring systems for any unexpected behaviour and adjust which accordingly.
6. The IT team documents the details of patching process into logs, reports on vulnerability & patch management activities to IT management then executives.
7. The executives (CISO) review the patch management process and consider updating policies if necessary.

#### 5.5.1.10.5 Identify Vulnerabilities and Their Patches

1. Utilise vulnerability scanning tools (e.g. Automox) that can automatically scan the systems, networks, and applications for known vulnerabilities and provide corresponding patches solutions occasionally. Frequently consult security advisories from the vendors of our hardware and software products or check industry-standard vulnerability feeds and databases (e.g. CVE) to further identify vulnerabilities and their patch solutions.
2. Conduct regular penetration testing (Holik et al., 2014) on networks and applications by our own IT team or hire external security experts. Engage with cybersecurity communities and professional networks through forums, online communities, and professional groups to obtain information related to vulnerabilities and their patches (while preserving organisational data triad).

# 5.6. Network Communications Security

The intended section presents an overview of the policies, regulations and control mechanisms related to the Network Infrastructure of the healthcare Centre, describing the purpose of the Organisation's adopted procedures based on risk assessment, Australia government guidelines and regulation and professional expert best practices.

## 5.6.1. Audience

This policy applies to all staff (healthcare professionals and management personnel), including temporary staff and contractors.

## 5.6.2 Introduction and Purpose

In a digital era, where digital data is the main asset in any business, network infrastructure is a key role for the workflow of information and business. As Rajamani and Iyer (2023) describe, the network is considered the backbone of any healthcare system.

In a healthcare Centre, could find different types of networks systems such as clinical support systems, physician collaboration networks, telemedicine networks, shared healthcare record access, and others, and these support networks ensure that systems provide data for critical decisions improving the quality of healthcare for patients (Rajamani & Iyer, 2023).

However, network interconnectivity, if not proper security policy, leads to several risks, since the network is the first entrance to healthcare systems. Cybercriminals and attackers can exploit vulnerabilities associated primarily with ICTs, causing data breaches of patients' confidential digital health information records (Zeadally et al., 2016).

The purpose of this section is to dictate the policies, procedures, and control mechanisms for assuring security and risk management of the Hospital's network architecture, using as guideline Health Insurance Portability and Accountability Act (HIPAA), and in compliance with the Privacy Act (1988) in Australia.

## 5.6.3. Network Policy Scope

This policy covers all aspects of network security, including but not limited to:
Network architecture, Access controls, Data encryption, Network Monitoring and Logging, Regulatory compliance (Network Security Policy - Template, n.d.)

- The network must be available when needed, and only can be accessed by authorised users.
- All sensitive data transmitted over the hospital's network, including patient health records, financial information, and administrative data, shall be encrypted using approved cryptographic algorithms and protocols.
- The hospital's network architecture shall be designed and maintained to minimise security risks, with segmentation and isolation of network segments to contain potential breaches and limit unauthorised access to critical systems.
- Network physical and virtual security resources shall be deployed strategically to monitor and control network traffic, detect malicious activity, and prevent unauthorised access.
- An incident response plan shall be developed, maintained, and tested regularly to ensure the hospital can effectively detect, respond to, and recover from security incidents affecting the network infrastructure

- The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality.
- It shall establish a periodical review of this policy to ensure compliance with regulatory requirements, with findings documented and remediation actions taken promptly to address any non-compliance issues.

## 5.6.4 Network Infrastructure Overview

### 5.6.4.1 Network Segmentation

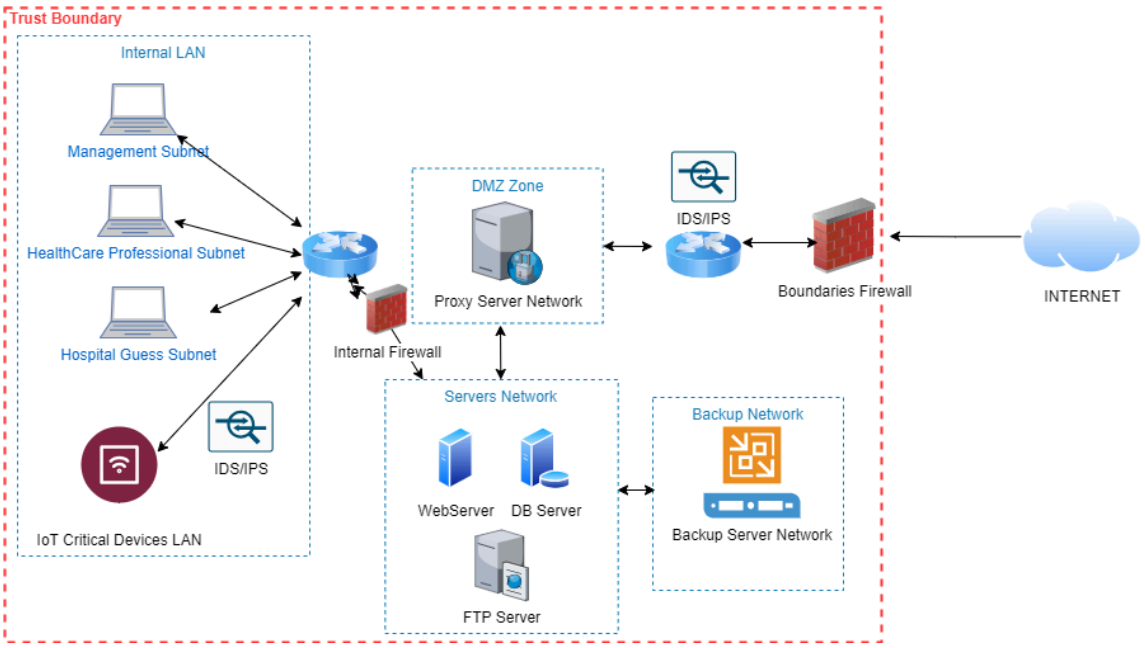
The network will be divided into smaller segments or VLANs according to the nature of the devices and/or system's functionalities. This action will allow independent configuration, management and scalability enhancing security and overall network performance (Ali, n.d.).

### 5.6.4.2 Network Design Diagram

The below image illustrates a high level of the Proposed Network Design including Network Segmentation proposal, Firewall, IDS/IPS functionalities (Akbar, M. S, 2024).

**Figure 3**

*Proposed Network Design*




*Note*. From INFO5301 Lecture Slides Week 3, by Akbar, M. S., 2024 Semester 1. Copyright by The University of Sydney School of Computer Sciences.

### 5.6.4.3 Encryption of In-Transit Data

- All in-transit data must be encrypted using the recommended encryption protocols and algorithms that meet current industry standards and recommended by HIPAA, to protect against unauthorised interception or eavesdropping.
- Transport Layer Security (TLS): All network communications, including email, web browsing, and file transfers, must use the latest TLS encryption to secure data transmissions over the internet and internal networks with a special consideration on critical exchange information processes where using mTLS is recommended (Rais et al., n.d.)
- Secure Sockets Layer (SSL): Legacy systems or applications that do not support TLS should use SSL encryption for secure communication.

- Strong Encryption Algorithms: AES (Advanced Encryption Standard) with a minimum key length of 128 bits or higher should be used for encrypting data transmissions.
- Encryption keys used for in-transit data encryption must be managed securely, following established key management practices.
- Encryption configurations should be based on HIPAA encryption requirements and recommendations provided by reputable cybersecurity resources.
- A strong Public Key Infrastructure (PKI) must be set up in order to properly handle encryption keys and digital certificates.
- A reliable Certificate Authorities (CAs) must issue certificates for Digital signatures, data encryption, and user authentication .

## 5.6.5 Network Monitoring and Logging

### 5.6.5.1 Access Control List (ACL)

- ACLs shall be implemented on all network devices in accordance with the organisation's security policies and access control requirements.
- ACL configurations should be documented, including details such as permitted and denied traffic, source and destination addresses, ports, and protocols. Documentation shall include test scenarios of ACL's changes (Chapter 7: The Foundation of Network Architecture, Part Two – Network Services - Network Architect's Handbook [Book], n.d.).
- Regular audits and reviews of ACL configurations should be conducted to ensure accuracy and effectiveness in enforcing access control policies.
- Least privilege principle shall be applied regarding ACL policies, where users are granted only the permissions necessary to perform their job functions.
- ACLs should be configured to enforce RBAC by restricting access to sensitive network resources and services based on predefined user roles or job responsibilities
- Any new ACL rule or modification shall be tested and validated to ensure it works as intended and the test shall include expected and unexpected traffic behaviour to identify any consequences of ACL implementations.

### 5.6.5.2 Monitoring Access and Network Devices Access Procedures

- Access control must be implemented by specified access procedures for network devices, such as switches, routers, firewalls, and other essential infrastructure components.
- For authenticating user's access network devices, access processes will incorporate multi factor authentication, usernames, and passwords.
- All access attempts, successful or unsuccessful, to network devices should be logged and audited to track user activities and detect potential security incidents or policy violations.
- Logging should include details such as the date, time, user ID, source IP address, accessed device, and actions performed during the access session.
- Privileged Access Management solutions shall be implemented to manage, monitor, and audit privileged access to network devices, including session recording and activity monitoring capabilities.

## 5.6.6 Firewall

- Firewall configurations shall be set to restrict access points between non protected systems (untrusted networks) and any system components in the protected healthcare information system.
- Also, internal firewalls will be set up to set boundaries between administrative network, server network and internal guest network for interexchange communication.

- All firewall implementations should adopt the principle of “least privilege” and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow permissible traffic (Murray, 2021).
- The firewall shall be configured to enforce default-deny inbound and outbound traffic policies, allowing only authorised communication based on predefined rulesets.
- Ingress and egress filtering rules shall be implemented to control traffic flow to and from external networks, with specific attention to blocking malicious or unauthorised access attempts.
- Regular firewall rule reviews and updates shall be conducted to adapt to emerging threats and address evolving security requirements
- The use of overly permissive firewall rules is prohibited (i.e., ANY/ANY/ALL rules).

### 5.6.7 Intrusion Detection/Prevention Systems (IDS/IPS) (Infosec, n.d.)

The procedures under the policy aims to detect and prevent unauthorised access, malicious activities, and security breaches:

- IDS/IPS systems shall utilise signature-based detection mechanisms to identify known patterns and signatures of malicious activities, including network attacks, exploits, and malware payloads.
- Signature databases shall be regularly updated to incorporate the latest threat intelligence and vulnerability signatures, ensuring timely detection and mitigation of emerging threats
- Behavioural analysis algorithms shall monitor network traffic patterns, user behaviour, and system activity to detect deviations from established baselines.
- Anomalous behaviour, such as unusual traffic volume, atypical communication patterns, or unexpected system interactions, shall trigger alerts for further investigation
- Shall be defined parameters for triggering IDS/IPS alerts based on the severity of threats, network sensitivity, and regulatory requirements.
- Designated IT personnel will conduct thorough investigations, perform forensic analysis, and implement remediation measures to mitigate the impact of the incident detected and alerted by IDP/IPS.

### 5.6.8 Security Email System

- Will be implemented email security gateways to filter incoming and outgoing email traffic for spam, phishing attempts, and malicious attachments.
- Shall be used encryption technologies such as Transport Layer Security (TLS) and S/MIME to secure email communications and protect sensitive information in transit.
- It will enforce email authentication mechanisms such as SPF, DKIM, and DMARC to prevent email spoofing and domain impersonation attacks.

### 5.6.9 Audit and Reviews of Network Control and Measurements.

- Frequency: Audits and reviews of the network infrastructure will be conducted at least annually or more frequently if deemed necessary.
- Documentation: Detailed documentation of audit findings and review outcomes will be maintained.
- An external audit will be led once every 2 years by a third-party to assure security controls are managed according to this policy.

## 5.7 Information Security Incident Management

The purpose of this Information Security Incident Management Policy is to establish procedures for detecting, reporting, assessing, and responding to information security incidents within the Australian Healthcare Centre. The policy is based on ISO/IEC 27001 standard to ensure the confidentiality, integrity,

and availability of sensitive healthcare data and critical infrastructure (Australian Signals Directorate, 2023).

### 5.7.1 Security Incidents Classifications

- Critical Incident: Security incidents that pose an immediate and severe threat to patient safety, healthcare services, or regulatory compliance.
- Major Incident: Security incidents that have a significant impact on hospital operations, patient care, or data confidentiality, integrity, and availability.
- Minor Incident: Security incidents with limited impact on hospital operations, patient care, or data security, but still require investigation and resolution.

### 5.7.2 Reporting an Incident

- All personnel, including healthcare professionals, management, and contractors must report any suspected or confirmed security incident to the designated Incident Response Team (IRT) or IT Security Department. This report can be via phone call, or email.
- Incident reports shall include detailed information about the incident, including date, time, location, affected systems or data, and any relevant evidence.

### 5.7.3 Incident Response and Assessment

- Once an incident report is alerted, the Incident Response Team (IRT) shall initiate the incident response process according to predefined procedures and protocols.
- The IRT shall conduct a preliminary analysis of the incident to determine its severity, impact, and appropriate response actions.
- According to incident classification, the IRT may escalate the incident to senior management, regulatory authorities, or law enforcement agencies.

### 5.7.4 Incident Containment and Mitigation

- The IRT shall implement containment measures to prevent the spread or escalation of the incident, such as isolating affected systems, computers, network segments, disabling compromised accounts, or blocking malicious network traffic.
- Mitigation strategies will be taken to address the root cause of the incident and restore normal operations in a timely manner.

### 5.7.5 Incident Investigation and Analysis

- A deep investigation will be conducted to find the cause, and impact of the security incident using investigative tools and techniques and in-written documents.

### 5.7.6 Incident Resolution and Recovery

- The IRT will design and execute a remediation plan to address the findings of the incident investigation and prevent similar incidents in the future.
- Shal bel prioritised the recovery and restoring affected systems, data, and services to their pre-incident state, with appropriate safeguards and security measures implemented.

### 5.7.7 Communication and Reporting Incidents

- Must be kept stakeholders informed about the incident status, response actions, and recovery progress via appropriate channels.
- Regulatory authorities, affected individuals, including patients, and other relevant parties shall be notified of significant security incidents in accordance with legal and regulatory requirements.
- Incident documentation shall be reviewed periodically to identify trends, patterns, or recurring issues that may require corrective action or additional controls
- Any changes to this policy must be approved by the corresponding group of authorities and must be notified to all personnel involved if required.

### 5.7.8 Acknowledgement

All personnel required to acknowledge and adhere to the policy.

### 5.7.9 Culture of Security

Promote a culture of information security and incident readiness.

# 6 Roles and Responsibilities

## 6.1 Chief Digital & Information Officer

Primary themes to the roles and responsibilities of the CDO and CIO are strategy, policy, risk, and budget (van Niekerk & Marnewick, 2024).

- **Strategy:** Monitoring the development and implementation of the hospital's digital and information strategy. Making sure that alignments with the goals and requirements of the hospital.
- **Policy:** Developing and enforcing information security policies and processes.
- **Risk:** Manage digital risks including identifying and assessing, to the hospital.
- **Budget:** Allocating resources for information security and managing the budget to support the digital infrastructures.

## 6.2 Information Owner

Information owners are typically responsible for the data's quality, integrity, and security.

- **Data:** Responsible for the patient data, employee information, and financial data's security and use.
- **Data quality and integrity:** Responsible for the data is accurate, complete, and reliable.
- **Access control:** Determines the range of who has rights to access and what can be accessed based on the principles of least privilege and need-to-know (Book, 2023).
- **Legal:** Making sure the data handling practices obey the legal, regulatory, and policy about data protection and privacy.

## 6.3 System Owner

System owners are responsible for the overall performance and functionality of specific IT systems within the hospital.

- **System configuration and maintenance:** Make sure the systems are configured securely updated and patched regularly.

- **Risk:** Regularly implement risk assessments of the systems, identify vulnerabilities, and control them.
- **Emergency plan:** Developing and testing contingency plans for system downtime and data breaches.

## 6.4 System Administrator

System administrators are technical experts, responsible for managing and operating the IT systems 24/7 (Terrell, 2021).

- **Daily management:** Daily operations of the hospital's IT systems such as installing, maintaining, and updating software and hardware.
- **Access control:** Implements the access controls to separate information owners and system owners.
- **Security Measures:** Installing firewalls, and antivirus software to protect systems from hacker threats.
- **Supports:** Technical support to users and staff on troubleshooting systems and network issues.

## 6.5 Information Security Team

The information security team needs to protect the hospital's information assets from any forms of threats and vulnerabilities (FCA, 2024).

- **Security Operation:** Manages security tools such as intrusion detection systems, encryption tools, and security information and event management systems.
- **Awareness and training:** All employees in the team need to be educated about security risks and best practices regularly.
- **Compliance:** Ensure compliance with standards (HIPAA) for healthcare data protection (United States Department Of Labor, 2004).

# 7 References


6clicks. (n.d.). *What are the 5 basic security principles?* | *Answers*. 6clicks. https://www.6clicks.com/resources/answers/what-are-the-5-basic-security-principles

Akbar, M. S. (2024, Semester 1). *Week 03 – Introduction to Network Security and Cryptography* [Image]. University of Sydney School of Computer Sciences, Information Security Management INFO5301.

Ali, A. H. (n.d.). Network Architect's Handbook. *O'Reilly Online Learning*. https://learning.oreilly.com/library/view/network-architects-handbook/9781837637836/

Australian Medical Association (2018, March 13). *AMA Guide to employment law for medical practices*. Australian Medical Association. https://www.ama.com.au/articles/ama-guide-employment-law-medical-practices

Australian Signals Directorate. (2023). *Guidelines for Cyber Security Incidents* | *Cyber.gov.au*. Australian Signals Directorate. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents

Best Practice. (2020). ISO 27001 Controls: What is Annex A:11?. *Best Practice.* https://bestpractice.biz/iso-controls-27001-what-is-annex-11/

Bhattasali, T., & Saeed, K. (2014, September). Two factor remote authentication in healthcare. In *2014 International Conference on Advances in Computing, Communications and Informatics* (ICACCI) (pp. 380-386). IEEE. http://dx.doi.org/10.1109/ICACCI.2014.6968594

Book, V. (2023, October 30). Least Privilege vs Need to Know in Cybersecurity. *Tufin*. https://www.tufin.com/blog/least-privilege-vs-need-to-know-cybersecurity

Colling, R., & York, T. (2009). *Hospital and Healthcare Security, 5th Edition*. Butterworth-Heinemann.

Croskey, C. & Terry, D. (2020, November 12). ACUA - Human Resource Operations: Internal Controls Practices and Risks for Pre-Employment Background Check. *Acua.org.* https://acua.org/College-and-University-Auditor-Journal/Fall-2020/Human-Resource-Operations-Internal-Controls-Practi

Data NSW. (2023, June 14). *Security classifications*. Data NSW. https://data.nsw.gov.au/nsw-government-information-classification-labelling-and-handling-guidelines/security-classifications

Edwards, M . (2023). Annex A.11 – Physical and Environmental Security. *ISMS Online*. https://www.isms.online/iso-27001/annex-a-11-physical-and-environmental-security/

FCA. (2024, April 12). *Role Of The Information Security Team In An Organization.* FCA - Financial Crime Academy. https://financialcrimeacademy.org/the-information-security-team/

Federal Register of Legislation. (2023, October 18). *Privacy Act 1988.* Federal Register of Legislation. https://www.legislation.gov.au/C2004A03712/latest/text

G, M. (2023, December 18). ISO 27001 Clause 1 Scope. *ISO Templates and Documents Download*. https://iso-docs.com/blogs/iso-27001-standard/iso-27001-clause-1-scope?_pos=3&_sid=4f2a87278&_ss=r

Gavrikova, E., Volkova, I. & Burda, Y. (2020). Strategic Aspects of Asset Management: An Overview of Current Research. *Sustainability, 12*(15), 5955. http://dx.doi.org/10.3390/su12155955

GDPR. (n.d.). *Complete guide to GDPR compliance.* GDPR. https://gdpr.eu/?cn-reloaded=1

Ghosh, D., Skinner, M. & Ferguson, L. R. (2006). The role of the Therapeutic Goods Administration and the Medicine and Medical Devices Safety Authority in evaluating complementary and alternative medicines in Australia and New Zealand. *Toxicology, 221*(1), 88-94. https://doi.org/10.1016/j.tox.2005.12.023

GNYHA. (n.d.). *SAFETY AND SECURITY CONSIDERATIONS FOR HOSPITALS.* GNYHA. https://www.gnyha.org/wp-content/uploads/2018/08/Security.pdf

Grove, A. (2019, February 19). Therapeutic goods: a quick guide. *Parliament of Australia*. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/rp/rp1819/Quick_Guides/TherapeuticGoods

Guard24. (2023, June 2). *The Importance of Hospital Security Guard Services*. Medium. https://medium.com/@hadu2486/the-importance-of-hospital-security-guard-services-b9f5118d6a07

Holik, F., Horalek, J., Marik, O., Neradova, S., & Zitta, S. (2014, November). Effective penetration testing with Metasploit framework and methodologies. In *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)* (pp. 237-242). IEEE. https://doi.org/10.1109/CINTI.2014.7028682

Hospital HR. (2023, October 16). *Scope of HR.* Hospital HR - Google Sites. https://sites.google.com/view/hospital-hr/nabh/scope-of-hr

Infosec. (n.d.). *Exploring Firewalls & Intrusion detection systems in network Security*. Infosec. https://www.infosecinstitute.com/resources/network-security-101/network-design-firewall-idsips/

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital healthcare-cyberattacks in Asian organizations: an analysis of vulnerabilities, risks, nist perspectives, and recommendations. *IEEE Access, 10*, 12345-12364. https://doi.org/10.1109/ACCESS.2022.3145372

Katarahweire, M., Bainomugisha, E. & Mughal, K. A. (2020). Data Classification for Secure Mobile Health Data Collection Systems. *Development Engineering, 5*(1), 100054. https://doi.org/10.1016/j.deveng.2020.100054

Keller, M. (2014). The art of enterprise asset management. *Journal of Digital Media Management, 3*(1), 23-30.

Kostadinov, D. (2020, July 20). Key Elements of an Information Security Policy. *Info Sec Institute*. https://www.infosecinstitute.com/resources/management-compliance-auditing/key-elements-information-security-policy/

Kosutic, D. (n.d.). What is ISO 27001? A quick and easy explanation. *Advisera.* https://advisera.com/27001academy/what-is-iso-27001/

Li, J., Mao, Y. & Zhang, J. (2022). Maintenance and Quality Control of Medical Equipment Based on Information Fusion Technology. *Computational Intelligence and Neuroscience, 2022*(1), 1-11. https://doi.org/10.1155/2022/9333328

Lindquist, M. (2023, March 23). The Importance of Healthcare Human Resources. *Oracle*. https://www.oracle.com/au/human-capital-management/healthcare-human-resources/

Linuhung, T. S. & Mediawati, E. (2023). Asset Management, Optimization of Asset Use, and its Effect on Local Own-Source Revenue. *International Journal of Business, Law and Education, 4*(2), 1475-1487. http://dx.doi.org/10.56442/ijble.v4i2.346

Liqing, L. & Hai, L. (2021). An access control model based on matrix domain security label. *Materials Science and Engineering, 1043*(4), 42046. https://doi.org/10.1088/1757-899X/1043/4/042046

Magnusson, F. (2018). Implementing a Backup-Scheme with the 3-2-1 Strategy: A Comparison of the Active Solution with a New Implemented 3-2-1 Backup-Scheme. *Mittuniversitetet*. http://www.diva-portal.org/smash/get/diva2:1246434/FULLTEXT01.pdf

Maya, G.  (2023). ISO 27001 - Annex A.11 - Physical and Environmental Security. *ISO Docs.* https://iso-docs.com/blogs/iso-27001-standard/iso-27001-annex-a-11-physical-and-environmental-security

Murphy, S. P. (2015). *Healthcare information security and privacy*. McGraw-Hill Education.

Murray, B. (2021, September 10). *Firewall policy*. University Policies. https://policy.uconn.edu/2021/08/30/firewall-policy-2/

Nikoloudakis, Y., Pallis, E., Mastorakis, G., Mavromoustakis, C. X., Skianis, C., & Markakis, E. K. (2019). Vulnerability assessment as a service for fog-centric ICT ecosystems: A healthcare use case. *Peer-to-Peer Networking and Applications, 12*, 1216-1224. https://doi.org/10.1007/s12083-019-0716-y

NSW Health. (2020). *Section 4 Legal & Policy Requirements Legal & Policy Requirements Legal Obligations for Health Organisations (p. Section 4.1)*. NSW Health. https://www.health.nsw.gov.au/policies/manuals/Documents/cgc-section4.pdf

NSW Legislation. (2023, October 1). *Health Records and Information Privacy Act 2022 No 71.* NSW Legislation. https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2002-071

NSW Ministry of Health. (2022). *Protecting People and Property NSW Health Policy and Standards for Security Risk Management in NSW Health Agencies*. NSW Ministry of Health. https://www.health.nsw.gov.au/policies/manuals/Documents/prot-people-prop.pdf

Paloalto. (n.d.). *What is IT Asset Inventory?.* Paloalto. https://www.paloaltonetworks.com.au/cyberpedia/what-is-it-asset-inventory#:~:text=The%20asset%20data%20stored%20in,%2C%20smartphones%2C%20printers%2C%20etc

Plachkinova, M. & Knapp, K. (2023). Least Privilege across People, Process, and Technology: Endpoint Security Framework. *The Journal of computer information systems, 37*(2), 1153-1165. https://doi.org/10.1080/08874417.2022.2128937

Rajamani, S. K & Iyer, R. S. (2023). Networks in Healthcare: A Systematic Review. *BioMedInformatics*, *3*(2), 391–404. https://doi.org/10.3390/biomedinformatics3020026

Rais, R., Morillo, C., Gilman, E., & Barth, D. (n.d.). Zero trust networks. *O'Reilly Online Learning*. https://learning.oreilly.com/library/view/zero-trust-networks/9781492096580/

Sandhu, R. S. (1993). Lattice-based access control models. *Computer, 26*(11), 9-19. http://dx.doi.org/10.1109/2.241422

Taylor, E. (2023). ISO 27001 - Annex A.11: Physical and Environmental Security. *The Knowledge Academy*. https://www.theknowledgeacademy.com/blog/iso-27001-physical-and-environmental-security/#:~:text=A.11.1.5%20Working%20in

Terrell, H. K. (2021, August). What is a system administrator?. *SearchNetworking.* https://www.techtarget.com/searchnetworking/definition/system-administrator

The Institute of Internal Auditors (n.d.). Physical and Environmental Controls. *Theiia*. https://www.theiia.org/en/products/learning-solutions/on-demand/physical-and-environmental-controls/#:~:text=Physical%20security%20controls%20protect%20assets

United States Department Of Labor. (2004). *Health coverage portability : Health Insurance Portability and Accountability Act of 1996 (HIPAA).* U.S. Dept. Of Labor, Employee Benefits Security Administration.

University of Newcastle. (2017). *Information Security Data Classification and Handling Manua*l. University of Newcastle. https://policies.newcastle.edu.au/document/view-current.php?id=256&version=2#section1

van Niekerk, T. & Marnewick, C. (2024). Who's who in the zoo? Clarifying the difference between the chief digital officer and chief information officer. *South African Journal of Information Management, 26*(1), 6–7. https://doi.org/10.4102/sajim.v26i1.1670

Woodley, R. (n.d.). Basic Security Principles. *Oracle Help Center.* https://docs.oracle.com/en/servers/management/hardware-management-pack-solaris/11.4/security-guide/basic-security-principles.html

Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security Attacks and Solutions in Electronic Health (E-health) Systems. *Journal of Medical Systems*, *40*(12). https://doi.org/10.1007/s10916-016-0597-z

# 8 Appendix (Justification of Exceeded Pages and Work Distribution)

In our dedication to providing a comprehensive information security policy for the healthcare organisation, we found it necessary to expand the document beyond the initial 15-page limit. We prioritise clarity and comprehensiveness in our policy to enhance understanding and make sure the guidelines are as detailed as possible. In our report, we specified the audience, purpose, and scope of each policy, as well as in-depth explanations of operational steps and the use of illustrative charts. We believe these additional pages could make the information security policy a more robust and reliable resource for the organisational operations to consult, thus reducing the information security risks.

**Work distribution:**
Andrea Aquino De Hoge - Network communications security, information security incident management
Henriette Elise Onarheim - Asset management, access control, formatting of report, references
Mingrui Xiao - Section 1 - 4, 6, human resources security
Ryo Nishiguchi - Physical and environmental security
Zekai Guo - Operations management