Hospital Network & Information Systems

Cybersecurity Manual

Guidelines, Recommendations and Awareness Training

ACKNOWLEDGEMENT

Many elements in this Cybersecurity Manual are inspired by and borrowed from guidelines provided within the document *Information Security Manual 2022* (cyber.gov.au 2022), published by the Australian Cyber Security Centre, under the Australian Signals Directorate.

Risk assessment, and risk management framework elements and processes are taken from the methodology recommended by the National Institute of Standards and Technology, NIST, (Guide for conducting risk assessments, 2012) and Risk Management Framework for Information Systems and Organizations (NIST, 2018).

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

Threats to networks and information systems range from designed attacks, human and machine errors, environmental instability, and structural or hardware failures, that can result in varying degrees of disruptions and harm to the operational or economic interests of the hospital.

This Cybersecurity Manual is tasked with providing strict security procedures, risk event handling, hardware/software security management guidelines, and policy directory. Awareness training and recommendations are also provided for hospital staff.

PURPOSE OF THIS DOCUMENT

This document outlines proactive and preventative measures that management and staff can undertake in managing risks and threat events, to protect the hospital's network, data, and information systems.

INTENDED AUDIENCE & USE

While this manual is intended for use by all hospital staff, it is primarily targeted at system engineers and management, containing strict guidelines for the designing, deploying, securing, and operational use of the hospital network, IoT Devices, and communication and information systems.

Senior management, network engineers and administrators, and the security department roles are largely responsible for designing, implementing, enforcing, and monitoring the cybersecurity recommendations and guidelines outlined in this manual. It is imperative that the hospital's organisational structure *at the very least* delegates this document handling through a role such as Chief Information Security Officer (CISO), empowered with dissemination and enforcement. Additionally, without exception, all staff members and third-party contractors working at/or for the hospital, are to undergo cybersecurity awareness training outlined within this document.

LEGAL CONSIDERATIONS

The hospital maintains compliancy with several legal responsibilities, including the Privacy Act of 1988 and 1996 (Australian Government, 2014), governing Patient Records, and Data Handling, and other privacy laws.

AUTHORITY

The Hospital Cybersecurity Manual draws authority of the subject matter contained within, primarily from the provided advice of the Australian Cyber Security Centre (ACSC) within their *Information Security Manual*. Other cybersecurity knowledge is procured from the advice given by respected authorities in their fields, referenced accordingly.

SCOPE

Due to the limited scope of the cybersecurity project, this document should be considered in an advisory role only, constrained by the theoretical nature of the expertise and knowledge professed by the students, which are employed in the researching, and preparing of this manual. That is to say that the author lacks real-life experience and authoritative knowledge.

CYBER SECURITY MODEL

RISK-BASED APPROACH, MODEL

The risk-based cybersecurity model, or Risk Management Framework (RMF), to be used as the guiding principle for the hospital cyber defence and protection preparations, is the NIST recommended RMF model *Risk Management Framework for Information Systems and Organizations*. The SP 800-37 Rev. 2 publication is used (NIST, 2018).

According to NIST "The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring".

In context of the hospital, a risk-based approach to network and information security allows the adoption of risk mitigating strategies that are unique to the hospital's operating environment. By leveraging the RMF, a systemic evaluation, identification and prioritisation of threat events facing the hospital was undertaken. This allows the ranking of threat events and associated risks, in order of importance, likelihood, and severity. For more details, please see the *Risk Assessment* section of this manual.

Microsoft Security defines the risk associated with a threat event or incident as "the impact of that incident multiplied by the probability of the incident happening" (Microsoft, n.d.).

In this way the hospital's network engineers, cybersecurity personnel, and administration can determine what cyber solutions are critical, make the most sense, provide the best protection, and return on investment.

RISK MANAGEMENT FRAMEWORK STEPS AND STRUCTURE

This risk-based approach for the hospital's cybersecurity is taken from the RMF framework, comprising of seven main activities as defined in the NIST guide, section 2.2 (NIST, 2018):

- **Define the System.** Prepare to execute the RMF from an organization—and a system—level perspective by establishing a context and priorities for managing security and privacy risk.
- **Categorise**. Categorise the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
- **Select controls.** Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
- **Implement controls.** Implement the controls and describe how the controls are employed within the system and its environment of operation.
- **Assess controls.** Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.

- **Authorise the system.** Authorise the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
- **Monitor the system.** Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

SECURITY ROLES FOR THE HOSPITAL

The hospital is expected to maintain a well-staffed cybersecurity department, overseen by the security leadership role of Chief Information Security Officer (CISO).

The CISO is charged with overseeing the hospital's entire cyber defence, in every aspect considered and implemented in the protection of the hospital's hardware, information systems, data, clients and personnel.

The CISO works with other specialists such as Chief Security Officer, Chief Information Officer, Cyber Intelligence Specialist, Data Privacy Officer, Information Security Analyst, IoT Security Specialist, IT Security Architect, Network Security Administrator, Security Auditor; and also consults with the hospital's administration, shareholders, HR department, legal department, and all other staff. In this way the CISO ensures that the cybersecurity program is run in accordance with the hospital's requirements, business goals, legal responsibilities, and unique threat landscape.

The CISO will take charge in cybersecurity reports and updates for senior management, and will also handle all incident response reports, and cyber breach incidents within the hospital and its systems. Security documentation such as plans, policies, controls, procedures, and recovery instructions, are also arranged through the CISO.

Finally, the CISO is also responsible for organising the budget and finances for the cybersecurity project.

GUIDELINES

This section gives recommendations and advice on all cybersecurity guidelines, implementations, and components related to the hospital network and use of its information systems and sensitive data.

Many of these guidelines are drawn from the guidelines provided within the cybersecurity document *Information Security Manual 2022* (cyber.gov.au 2022), and from the results of the Risk Assessment done for the hospital, and the resulting Policies that were created thereafter. Other guidelines are drawn from industry recommended cybersecurity best practices and standards.

HOSPITAL NETWORK GUIDELINES

The network design is planned down to every minute detail required to produce accurate architectural diagrams, that are manifested in physical reality. In-depth network documentation is also provided, to assist in securing and maintaining a healthy network, and troubleshooting network problems.

As identified in the risk assessment conducted for the hospital systems, the network design must be stringent in combating threat events that would cause significant downtime for the network, and the hospital's infrastructure. To assist with this, reliability and security requirements associated with the smart network are also implemented. Ransomware poses a huge threat to any network should there be an infection. The network implements regular backups of all data to an offsite backup server, and cloud-based backups.

Hacking prevention systems are included in the design of the network in the form of intrusion detection systems, and network anomaly detectors are utilised to maintain a safe network. Logging in to the network by IT administrators is also regularly conducted, as well as separating the network to avoid deeper penetration hacking attempt. All servers are maintained with the most up-to-date software, with a policy of patching major vulnerabilities within 24 hours. This provides a dramatic reduction in both hacking and virus-based attacks.

Network Design

The network design is provided as high-level network diagrams showing all endpoints and connections into the network. Logical diagrams illustrate all the critical components such as servers, high value hardware, network devices, and security appliances.

Both the network design and documentation also provide illustrations and instructions pertaining to network security, intrusion prevention, defence mechanisms, incident recovery, and all the aspects of cyber defence that are implemented within.

The following guidelines are core in delivering the hospital network:

I. **Network segmentation and segregation.** This is a very important and effective way to prevent unauthorised users, criminal adversaries, from propagating access throughout the system once they have penetrated it. Each segmentation requires additional authorisation and conditions to gain access, additionally protecting infrastructure such as administrative services, sensitive databases, hospital medical devices, and patient care systems.

II. **Network encryption.** All communications made over the network use encrypted protocols. Every packet set is secured against unauthorised prying.

III. **Network access controls**. Network access controls prevent unauthorised physical access to the network, and threats accidently introduced by improper bridging and connecting of sub networks with the hospital, from hospital staff. NAC also acts as network limiter, restricting the flow of traffic where desired.

IV. **Domain Name System Services.** DNS will block unwanted or unauthorised requests within or to the hospital network, of known malicious domains and IP addresses. Filtering and logging of DNS requests helps security monitoring and auditing.

V. **Separation of servers:** Separating critical server types and roles from each other, and even segmenting them, reduces the chance that one compromised server can be used to penetrate others. Recovery and healing of a compromised server is also simplified.

VI. **Network traffic management.** Using network hardware such as firewalls, iptables, aids in the strict management of traffic within the network. This additional security reduces adversarial connectivity and movement within the network, and restricts gathering network information such as hosts, devices, groups and usernames, and other sniffable network-related data.

Wireless Network Design

The wireless network design also provides high-level wireless network diagrams showing all endpoints and connections into the network. Logical diagrams illustrate all the critical components such as access points, firewall hardware, network routing devices.

Wireless documentation also provides instructions pertaining to network security, intrusion prevention, defence mechanisms, incident recovery, and all the aspects of cyber defence.

The wireless network allows the hospital’s many IoT devices to connect seamlessly within the network, supporting the core services required for staff duties and patient care. Key areas of WIFI needs are identified and provided optimal security, within the hospital floor plan. The need for EMF protections are also considered in the wireless network, for example the radiology, MRI and X-ray areas are equipped with WIFI blockers/walls to ensure WIFI signals do not interfere with medical devices, while the cafeteria, ICU, and lobby/waiting areas will ensure a mix of public and private WIFI is available. Keeping these networks separate ensures ideal security for the network.

The following guidelines are core in delivering the wireless network:

I. **Wi-Fi Alliance Certified.** All wireless devices are certified through the Wi-Fi Alliance certification program. This includes wireless access points, boosters, adapter cards, and network cards. This standard guarantees greater security and interoperability of the wireless network and devices operating within.

II. **Non-Default settings.** The default settings of wireless access points are usually weakly configured. Access points and devices typically use Service Set Identifiers (SSIDs) account settings and credentials, that are all securely reconfigured for the hospital.

III. **802.1X authentication.** The wireless network uses WPA3-Enterprise 802.1X authentication, using the Extensible Authentication Protocol (EAP). Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) provides strong security benefits. WPA3 is considered the most secure commercial wireless encryption standard.

IV. **Media Access Control address.** All devices connecting to the hospital's wireless network such as medical equipment, patient wearable IoTs, personnel devices, environmental and security sensors, are permitted and controlled according to their MAC address. This insures only legitimate devices gain access.

V. **Patient WIFI segmentation.** Wireless connectivity for patients is provided in limited areas and is fully separated from the main hospital wireless network thus preventing intrusions and attacks on critical systems. Use of this public WIFI is also restricted to limited domains and services, use is monitored and logged, and traffic bandwidth is limited.

Network Redundancy

In the event of a disaster (hacking (DDOS), ransomware, hardware failure, natural disaster), for the hospital network an integrated redundancy design will mitigate severe impact and provide a more consistent reliability and availability of the network.

Partial or full network failure was classified in the risk assessment report as a medium potentiality/high impact risk event. Implementing network redundancy considerably reduces the potential of a failure event. For the hospital network, backup servers and routers are positioned to take the load in the case of critical failure or system instability, acting as a failover provision. Network redundancy can also incorporate elements such as a distributed network approach that leverages VLANS and load balancers.

Firewalls, Antivirus

Hardware Firewalls

The hospital network implements hardware firewalls between the outside world and the local area network. Additional firewalls are placed within the network, acting as gateways between the various segmented network portions. This protects against outside intrusions, and cross domain intrusion within the local area network. These firewalls monitor all incoming/internal/outgoing network traffic, blocking or allowing it by using pre-defined security and routing rules. Splunk and SolarWinds are integrated to assist in the management of firewall rules, monitoring, and behavioural analysis.

Software Firewalls

As an additional layer of active protection, software firewalls are utilised at the application level. Hardware firewalls are not impervious, so software and operating system firewalls provide an additional fallback. Acting like an umbrella, software firewall protects against malicious code execution that takes advantage of vulnerabilities in common network protocols such as HTTP, HTTPS, SMTP, DNS, and open ports. McAfee enterprise firewall provides end-to-end device protection for the hospital.

Antivirus software

Antivirus software is to be installed on all devices that have application-level capability, protecting against a large range of known viruses, malware, trojans and other types of malicious code that exploit known vulnerabilities in the software and operating system required to carry out the hospital's operations and services. McAfee enterprise antivirus also provides cloud-based services scanning.

Cabling infrastructure

Fibre-optic cables

Throughout the hospital, Fibre-optic cables are used where possible. Fibre-optics don't produce electromagnetic emanations and cannot be tampered or affected by them. This prevents electronic sniffing and intercepting attacks, providing the highest degree of protection from electromagnetic emanation threats.

Cabling standards

Australian Standards for network cabling and infrastructure are complied with, along with the employment of certified cable installers and network engineers. All the cabling and related hardware components that make up the network are up to code, providing the best quality, throughput, stability, availability, and security of the system.

Additionally other cabling needs for the hospital are also governed by Australia Standards and regularly inspected by quality electricians, such as:

- Medical equipment and machinery
- Patient beds and monitoring equipment
- Fire and alarm systems
- Security and control systems
- Telephone and voice systems
- Lighting control systems

Cable Maintenance

In order to maintain, inspect and correctly handle the network's myriad of cables and assisting connecting devices, a well-documented labelling process is used. Cable registers, cable deployment diagrams, floor plan diagrams, network diagrams, and electric architecture diagrams are used to assist in the installation and maintenance of the extensive cabling.

Regular inspections are to be carried out by qualified IT staff, and where necessary by electrician inspectors, recording and tracking the cable ecosystem over time, replacing aging portions, and upgrading where necessary.

Availability of Internet

The day-to-day operations of the hospital rely on several important services that use technologies that are dependent on internet connectivity and cloud services. Importantly, the hospital uses optic-fibre internet service providers that provide connections which meet the sizeable bandwidth, download and upload speed requirements. Low latency, high reliability, and nonstop availability are also crucial. Several providers are to be sourced, including mobile and 5G variants, and redundant internet connections, for failover purposes.

Denial of service protection

Denial-of-service (DOS) attacks are frequently targeted at larger organisations, with hospitals often targeted. Distributed DOS attacks are intended to disrupt, degrade or cripple the targeted website or service. In this state the attackers may demand a ransom to cease, or further penetrate or sniff the system while it is in awakened state. The hospital uses many services that can be targeted by DDOS attacks, so is proactive in defending against them. Several mitigations are leveraged such as the use of Content Delivery Networks, distributed load balancing, web response caching, domain name registrar locking, and cybersecurity tools that use real-time monitoring and mitigation of DDOS attacks.

Separating critical services that require internet or cloud connectivity

Services that are critical to the lifesaving operations of a hospital, patient care, and security, are segregated and hidden on the network and provided with separate internet connections that won’t be affected by DDOS attacks that occur on the more visible network surface areas.

IoT & EQUIPMENT GUIDELINES

Network Hardware & ICT Equipment usage, maintenance, and disposal

Equipment registers

A regularly maintained register is kept of all hardware and ICT equipment within the hospital. This provides a way to track and organise all legitimate ICT equipment, and detect unauthorised equipment introduced into the system. Equipment can also be monitored for aging and upgrade potentiality. This equipment audit ledger also assists in the business operations of the hospital, accounting, and financial evaluations. The network registered devices such as workstations, servers, routers, cables, APs, communication equipment, and connected medical machines and IoT devices are all recorded in this ledger.

Classification and Handling

The equipment must be classified, to determine and acknowledge the sensitivity and classification of the data that is processed and/or stored on its media. An ICT equipment management policy will govern how all equipment is classified, handled, and disposed of. Some ICT equipment and IoT devices requires data encryption technology, special permissions, and specific handling rules.

Equipment sanitising

When equipment is sanitised, all media and sensitive data must be destroyed as per this policy. Documenting this decommissioning of equipment and storage media is also required, for auditing and forensic purposes.

Media typically found in ICT equipment includes (cyber.gov.au 2022):

- electrostatic memory devices, such as laser printer cartridges used in multifunction devices (MFDs)
- non-volatile magnetic memory, such as hard disks
- non-volatile semiconductor memory, such as flash cards and solid-state drives
- volatile memory, such as random-access memory sticks.

SOFTWARE GUIDELINES

Software procurement

Working with suppliers

The CISO in charge of cybersecurity for the hospital is responsible for ensuring consistent software procurement, management, and upgrade services.

Third-party software and services, and relationships with their developers/vendors presents additional security risks. The job of the CISO is to assist IT personnel in assessing such cyber supply chain risks and the security threats resulting from the use of the software and the conditions of the contracts with the suppliers.

Software security evaluation

An evaluated product provides a level of assurance in its security functionality that an unevaluated product does not.

By using software and applications that have been evaluated for security vulnerabilities and risks, the hospital gains an additional level of protection against threat events that could compromise or cripple information systems from the inside.

The hospital CISO and IT cybersecurity personnel charged with evaluating software can employ the Australian Cyber Security Centre (ACSC) to perform official software evaluations with the following services (cyber.gov.au 2022):

- Australian Signals Directorate (ASD) Enterprise Mobility Evaluation Program: For enterprise mobility products used to protect sensitive or classified data.

- ASD High Assurance Evaluation Program: For products used to protect SECRET and TOP SECRET data.

Verify software integrity

It is critical that official and updated versions of all software are used, by downloading them from the official supplier provided locations, and then verified by their checksum, before introducing them into the hospital network. Programs such as Microsoft FCIV can assist in this process, and as this is a CLI utility, it can be deployed and accessed quickly by system administrators.

Software Management

The CISO and approved cybersecurity staff, such as system administrators and information system specialist, are tasked with software management.

Management installation privileges

Only the approved hospital personnel can install applications and software, being provided with roles and permissions that only allow them to execute the installation processes. Furthermore, only authorised personnel can uninstall or modify existing programs, preventing the removal or compromise of services and security software. Certain enterprise software, or critically important and data sensitive software are guarded with additional access controls, only allowing access, and setting configuration changes by authorised personnel.

Monitoring and control

Access controls and logs also provide records and audits for all illegal attempts to install software, and unauthorised installations. Uninstallation and configuration changes are also monitored, including metrics of user, time and place.

Software use privileges

Based on their role at the hospital, users will only be authorised to access certain parts of sensitive applications. For example, Administration staff will not be able to enter any patient observation or diagnosis notes, but will be able to add and edit patient contact details and staff contact details and accounts.

Patching Software

Typically, the updated and patched versions of software used by the hospital is more secure than the older versions. System administrators and the CISO keep track of all installed software in a registrar, and the current versions available by their suppliers. If there is sufficient reason to upgrade, then this is undertaken, by first testing and deploying the new versions of software in a development environment to determine their stability and capability, then integrating or patching them into the live hospital systems.

CORE SECURITY GUIDELINES

The following guidelines describe the main network, operational data, and information security elements implementable within the hospital's systems, that greatly reduce vulnerabilities and security risks of the network, patient health data, and information systems.

Network and Information Security

Physical security

Preventing physical access to critical infrastructure will help close a number of attack vectors, such as the installation of snooping devices (network sniffers, keyboard loggers), the installation of malicious software, physical damage/destruction of devices, theft of devices, sabotage of devices, etc.

Proxy Server

A proxy server provides an extra layer of security by preventing the exposure of internal IP Addresses to the internet and play a role in other security measures such as content and URL filtering.

Firewall

The firewall is a critical security element, monitoring network traffic, using pre-defined rules to block unwanted communications including those that may be associated with viruses and other malware, and hackers. A firewall that monitors both incoming and outgoing traffic will help reduce the risk of attack from outside the network and from inside the network.

Intrusion Detection System

An intrusion detection system uses data collection and analysis of network traffic to identify if an attack is in progress. The system can use signature-based detection, where network activity is compared to known cyber-attack activity and anomaly-based detection where machine learning is used to identify activity that is outside of the normal baseline activity of the network. If the system identifies a potential threat, an alert is sent to appropriate members of the IT team and other departments/management as required.

Intrusion Prevention System

An intrusion prevention system extends the function of an intrusion detection system by adding the ability to intervene to prevent attacks that are detected through methods such as dropping packets and connections, and blocking IP addresses.

Content Filtering

Using pre-defined rules, prohibited content is blocked from entering the network.

URL Filtering

All traffic from a list of prohibited websites is blocked from entering the network.

Least Privilege Doctrine

The principle of least privilege is that every user, account, script, automated system, etc., in the system is only given the lowest privileges possible while still allowing the completion of the jobs, tasks, function, etc., they are assigned. This approach helps to prevent system disruption due to unwanted user changes, data protection by restricting access to the minimum required, and mitigating damage in the event of a successful attack by limiting the parts of the system accessible by compromised entities.

Access Control

Access control is a key pillar of network security, it allows users to access data and systems they have permission to and prevents anyone without permission from accessing data and systems.

Authentication

Authentication is the method by which a user identifies themselves to the system, commonly this is done using a username and password but due to the flaws inherent in this method, multi-factor authentication such as one-time security codes, smart cards, biometric data, etc., should be used where possible, particularly for highly sensitive data and systems. Unauthenticated users should not be able to access any part of the network.

Authorisation

Authorisation is used to control which authenticated users can access which data and systems. Each resource has a list containing authorised users and all other users who are prevented from accessing it.

Anti-malware System

This software installed on network devices is designed to detect the presence of malware. The system will be made of multiple components, a “shield” which will attempt to detect malware as it is downloaded, run, or accessed in any way, and a scanner which scans the system, using known malware signatures and other analytical methods to identify any potential malware.

Security Policies

Security policies are another vital security element, they provide clarity and consistency for IT staff when designing, implementing, maintaining, and administering the network. Security policies are also vitally important as a guide to other staff. Users are some of the most exploitable attack vectors into a system and well-written security policies are vital in educating staff, encouraging good behaviours and eliminating bad behaviours. Additionally, backup and recovery procedures are a crucial part of the plan to return the network to an operational state after a catastrophic failure.

Network Security Auditing

Regular audits of network security are vital to identify and resolve previously unnoticed vulnerabilities, issues arising from newly discovered exploits, unsafe practices which have become common and any other issues which may arise.

Data Encryption

Data is vulnerable when it is stored and when it is in transit; by using modern, effective encryption technology and techniques, data can be protected from unauthorised access and alteration in both these states.

Data in transit, between the client and the server, is protected with Transport Layer Security (TLS) Protocol enabled authentication, encryption, and verification. The creation of secure TLS socket connections is achieved using the Java class SSLSocket which uses digital certificates to authenticate the client and the server, and uses encryption keys and ciphers to encrypt the data to prevent snooping, theft and tampering while it is being sent between the client and the server.

Password Encryption

The passwords of ordinary users of the application will be stored in the database, thus protections need to be put in place, so that if an attacker does gain access to the system, perhaps by phishing the credentials of a user, that attacker cannot move laterally through the hospital by learning the passwords of other users which may have higher permissions or access to different resources.

For all logins that connect to locally hosted password authentication services, a hashing of the passwords is performed by the application in use, before any password is sent to the database, so the database does not see any user’s application password in clear text. The application uses the PBKDF2 key derivation function as mentioned above, to transform passwords for safe storage. Once the key derivation function has completed, the resulting password hash and the randomly generated salt are stored in the database.

Network Segmentation

Network Segmentation, the dividing of a network into smaller portions, either physically or logically is a way to mitigate the impact of attacks and other security issues. Without segmentation, devices can communicate with each other easily which provides convenient access for an attacker to move from a compromised machine to the entire network. By using segmentation, the portion of the network which can be easily accessed is greatly reduced, network traffic between segments must go through network devices such as routers and firewalls, and be subjected to firewall rules, access control and other security implementations which make it much harder to spread throughout the network. Given the highly sensitive and critical nature of many hospital systems, for example patient records, intensive care systems and surgical theatre systems, segmentation will be an integral part of the hospital network.

Demilitarized Zone (DMZ)

One form of network segmentation is a DMZ. Any portion of the network that needs to be accessible externally is put in the DMZ and only the minimum required resources are included, external access to all other parts of the network is blocked.

Network IoT Security Components

Hospitals are increasingly a target for cyber-attacks, coupled with the growing concern of the vulnerabilities and risks in IoT, preventative and reactive security measures are strongly incorporated.

The protection of IoT devices will be provided by both the hospital network security, and AWS IoT security components (for devices integrated into the cloud). Physical security is also considered, along with user policies, and auditing mechanisms.

Encryption and Cryptography

Encryption and cryptographic security are used for all IoT device communications. The Transport Layer Security (TLS) 1.2 protocol is used along with the X.509 certificates. Amazon Web Services IoT Core facilitates the creating and registering of X.509 certificates, to securely authenticate all the medical IoT devices integrated into the AWS cloud. A private and public key pair is also generated for each registered IoT, allowing asymmetric cryptography. RSA and SHA algorithms are supported, up to 512bit keys. Full certificate support is available, including expiration and reissuing management, and Certificate Authority handling.

IoT devices are additionally protected with AWS Darktrace AI and AWS IoT Defender to monitor and audit their state and communications for anomalies and suspicious behaviour. Behavioural metrics are used by Machine Learning assisted AI security to detect and prevent malicious IoT behaviour.

SECURITY INCIDENT GUIDELINES

In the event that a suspected or verified breach has occurred in a hospital system, service, or network, an official cybersecurity incident report must be filed and investigated by the appropriate hospital personnel.

Each head of department is responsible for working with subordinate staff in filing incident reports. Reports must be filed without delay, using the centralised incident reporting service provided by the cybersecurity department.

The Chief Security Information Officer (CISO) is responsible for dealing with all incident reports in an immediate manner, delegating the investigation, mitigation, and healing processes. Serious incidents are further reported to the CEO and hospital board.

Managing incidents

The hospital's CISO is tasked with arranging the development of an incident response plan that is executed whenever a cyber incident occurs, allowing personnel to respond quickly and appropriately. The response plan prevents cybersecurity incidents from escalating and directs the restoration of impacted systems. Digital forensics is used to preserve any evidence.

This incident management plan proves a proactive response against current and future incidents, increasing the detection, handling and mitigation of threat events. According to the ASD, incident management should cover (cyber.gov.au 2022):

I. Responsibilities for planning for, detecting and responding to cybersecurity incidents.
II. Resources assigned to cybersecurity incident planning, detection and response activities.
III. Guidelines for triaging and responding to cybersecurity events and cybersecurity incidents.

Handling, Logging, and Reporting Incidents

Incident register

The CISO provides a well-maintained security incident register of cyber incidents. This register assists with incident remediation and management. Recorded within are the types of cyber incidents, their frequency, severity of the breach, and costs of any correctional activities. This information is used for future risk assessment and auditing activities.

Handling intrusions

Active and ceased intrusions to the system are handled by cybersecurity personnel. The CISO develops an IDS and IPS policy and procedure to handle such events. Intrusions with limited effect may be allowed to continue to understand their nature, whilst intrusions that will breach legal compliancy, such as expose confidential patient records, are destroyed with a prejudice. AI-assisted intrusion prevention systems operate autonomously and will automatically shut down all detected events.

Handling malicious code and data infections

Whenever any malicious code is detected in the system, the critical first step is initiated in quarantining and removing the virus, malware, or compromised file/data. All infected systems and media are to be isolated, and the malicious code contained, limiting the system damage and exposure of confidential or sensitive information.

The infected portion can then be dealt with, using proper antivirus remedies, malicious code removal tools; or in severe cases the affected system or databases will be formatted and reinstated back to a previous state of backup.

Handling infection spills

In the event that malicious code spreads from the initial location, or infected data spillage occurs, a code red is initiated by cybersecurity in accordance with the hospital's Incident Management plan, and the affected systems are either powered down in severe circumstances, and/or the internet and LAN connections are disconnected. Segregation of the affected network/system must be enacted immediately. Then the process of forensics and auditing, cleaning, and restoring can be undertaken.

Preserving integrity of evidence

Cybersecurity and network administration personnel should be trained in the proper procedures in identifying, gathering, and preserving digital forensic evidence. The Australian Cyber Security Centre (ACSC), and certain Australian government agencies provide such guidelines, and may be requested to assist with investigations of a serious nature. The ACSC is very helpful in aiding organisations in dealing with serious cybersecurity incidents, suggesting that the following events be reported to assist in the development of future cybersecurity advice (cyber.gov.au 2022):

- suspicious activities, such as privileged account lockouts and unusual remote access activities
- compromise of sensitive or classified data
- unauthorised access or attempts to access a system
- emails with suspicious attachments or links
- denial-of-service attacks
- ransomware attacks
- suspected tampering of ICT equipment.

DATA GUIDELINES

In the event of a critical data loss (through hacking, ransomware, personnel mistakes, hardware failure, or even natural disaster), the following backup approach can prevent data loss and expediate any recovery processes in an actual event such loss occurs.

Hospitals utilise a large amount of third-party provided data, through the cloud and partner data server solutions, for the daily operational tasks of personnel and services. From electronic health records, treatment protocols, drug information databases, to research material and financial services.

However, an enormous amount of data is generated, transmitted, and stored locally, that is private and required to be secured and backed up. This ranges from hospital-specific patient record details, treatment and prescription data, clinical data, trials and research data, administrative data, to patient intake and outtake management, and the massive amount of recordable data generated by IoTs and other medical devices.

Database servers, DBMS

To protect the data stored in the database, multiple security measures are put in place at the database level, such as at-rest encryption, user account control and password storage best practices.

DBMS encryption

MySQL DBMS has the in-built capacity to encrypt all data stored in a database. With the correct settings, MySQL will encrypt data as it is saved and decrypt it as it is read, so that if an attacker gains access to the server and attempts to read the data from storage, it will be encrypted and unreadable. While at the same time, accessing the data legitimately through MySQL is transparent, no extra steps or accommodations are required to account for the presence of encryption. Additionally, all communication between databases and the hospital's web servers is also encrypted.

User account control

User account control will be used to control who can access the database and what permissions approved users are given to perform tasks such as adding, editing, deleting data, altering table/database design, and deleting database elements. As a result of the application architecture, ordinary users will not have direct access to the database, rather the server application process will connect to the database using an account with only the minimum permissions required to perform the tasks an ordinary user would be doing.

Database server and web server separation

All databases that host sensitive patient data, and hospital operation data, are segregated from any servers that are exposed to the public such as the hospital's web servers. Functional separation of the database servers from the more vulnerable servers greatly reduces the security risks and possibility of being compromised by threat actors.

Database segregation

Databases holding sensitive information are located on separate network segments that all the hospital's IoTs and workstation devices are located on. This functional separation of database servers and the network portions where personnel are connected to, reduces the security vulnerabilities and possibility of being compromised by insider sabotage, or risky behaviour that leads to cybersecurity incidents.

Database event logging

Many database events and requests assist the cybersecurity monitoring and behavioural analysis of the hospital's databases. Live logging facilitates in detecting malicious data requests, SQL injection attacks, privilege abuse, and misconfigurations. Database event logs are centrally stored and guarded against modification and unauthorised deletion.

Database hardening and proper configuration

Improperly configured databases are a self-inflicted vulnerability that is commonly exploited by attackers. The hospital databases do not use default account, permission, and configuration parameters. Databases are configured with strict settings, permissions and access rules, strong audit trails, dynamic backlog mechanisms, encryption protocols, and are further secured with IDS monitoring technologies. DBMS installation files and logs are also removed after installation.

Backup and redundancy

The hospital depends on services that require uninterrupted access to and use of confidential and sensitive data, patient health records, financial information, drugs and treatment data, research data, and so on. The hospital network and DBMS can take snapshots of current databases and server states, to seamlessly backup and restore them.

Data backup and restoration

A database backup and restoration plan are implemented, supporting the availability and integrity of data needs by the hospital. Backups are run using various technologies like tapes, backup media, duplicate database mirroring, and cloud service backups for selective data.

Backups are run in cyclic intervals or in a constant mirrored state, depending on the database and the critical nature of the servers. All network supporting servers and databases are backed up daily, hospital personnel workstation data is backed up regularly, and all data that is in constant motion (financial records, patient records, treatments, medical device data, tests, diagnosis, research) is backed up live, using distributed and/or mirrored databases, and cloud backups.

The data restoration process supports the disaster recovery planning, incident management planning, and the healing and restoring process post cybersecurity incident.

Backup access and permissions

The backup technologies, backed up images and files, and physical media containing backups, are protected from unauthorised access. In all states of backup, without the correct permissions or access authority, users cannot access, modify, or even delete backups. This preserves the data's confidentiality, complies with privacy laws, prevents malicious access and compromise, and criminal attempts to destroy evidence.

Backup testing

To ensure backups are usable and can restore the required data with full integrity, it is critical that the CISO or system administrator tests the backups. A yearly review of the hospital's backup procedures, storage handling, security and legal aspects, and backup testing, should be conducted.

COMMUNICATIONS GUIDELINES

An email usage policy has been created to give guidelines for the hospital personnel as numerous security risks are related to the use of email services.

EMAIL usage, Gateways, and Servers

Webmail services

Access to webmail services that haven't been approved by the hospital should be blocked to mitigate potential risks due to their un-evaluated security standards.

Protective markings

Appropriate protective markings should also be utilised to ensure that the security status of email bodies and attachments is reflected to those handling the information. Email servers must be configured to block emails that have inadequate protective markings.

Email content filtering

Content filtering should be performed on email bodies and attachments to prevent malicious code from being introduced into the hospital network.

Blocking suspicious emails

Suspicious emails should be blocked to mitigate the possibility of phishing emails entering the hospital network.

Email gateways

It is more efficient and secure to route emails via centralised email gateways to deploy DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, and Sender Policy Framework (SPF). To prevent malicious activities, backup and alternative email gateways should be maintained at an equal standard to the hospital's primary email gateway.

Email server TLS encryption

To mitigate the risk of emails being intercepted between the originating email servers and the destination email servers, the hospital's email servers use the encrypted Transport Layer Security (TLS) protocol. However, as TLS encryption can be susceptible to downgrade attacks, Mail Transfer Agent Strict Transport Security (MTA-STS) is also used to ensure that email transfers only occur if the TLS encryption is satisfactory.

DomainKeys Identified Mail

DKIM facilitates the detection of malicious email spoofing by verifying the digital signature linked to a domain name in an outbound email. If the signed digest contained in an email header doesn't match the signed email contents, then the email authentication will fail. The hospital email management must also incorporate the DKIM component.

Telephone, Mobile Device usage

Mobile device usage

A mobile device management policy is implemented to ensure that mobile devices that leave the protective hospital environment continue to be used in a secured manner.

Privately-owned mobile devices

Hospital personnel that use privately-owned mobile devices to access the hospital's databases and patient data, can present a major security risk. Thus, the hospital CISO needs to determine if the increased liability risks are acceptable, and if they are compliant with the relevant legislation, such as the Privacy Act 1988 and the Archives Act of 1983.

Storage encryption

A mobile device's internal storage, including any removable media, should be encrypted to prevent an adversary from accessing sensitive or confidential data if the mobile device gets lost or stolen.

Communications encryption

Mobile devices communicating data that is sensitive or confidential will pose a security risk if appropriate encryption is not used to protect the data in transit. All applications and services that transmit data from the mobile phone, must be evaluated, approved, and utilise adequate encryption protocols.

Mobile device security

Hospital personnel should initially be provided with secure mobile devices and their security must be maintained overtime. Hospital personnel should not be allowed to install/uninstall applications that have not been approved, or modify/disable security functions on their mobile devices. These devices are strictly "work-only" and must also be monitored by central security. End-point firewall and antivirus software is to be installed and maintained, such as McAfee.

Connecting mobile devices to the internet

When connecting a mobile device to the internet, a Virtual Private Network (VPN) connection to the hospital's internet gateway should be established rather than connecting directly to the internet. In this way, mobile devices will benefit from additional protection and security, such as web content filtering. Additionally, critically sensitive applications and services within the hospital will not allow remote access connections, or connections from mobile devices and work-from-home devices.

Maintaining control of mobile devices

Mobile devices can easily be lost or stolen due to their portable nature, so hospital personnel must supervise them continually and store them securely. Remote access/wipe technology set up by the cybersecurity department can be used to delete or sanitise data on mobile devices in the case of theft or loss of the device.

Telephone devices usage

Hospital personnel should not communicate information that is sensitive or confidential over a public telephone system that is unsecured and susceptible to interception.

Protecting conversations

While sensitive or confidential information is communicated over telephone systems, the conversation must be adequality protected with the use of encryption during the call.

Cordless telephone systems

Cordless telephone systems should not be used as they offer very little transmission security and are easily subject to interception. This can result in disclosure of sensitive information to a threat actor engaging in a type of MITM attack, or unauthorised third-party.

Fax or MFD usage

Adequate encryption

Only approved fax and MFD hardware that uses adequate encryption protocols is permittable. Once it has been connected to a cryptographic device and utilised to send a sensitive message, a fax machine or MFD cannot be trusted when connecting directly to telecommunications infrastructures which are often unsecured in-between. The telecommunication system needs to be correctly classified and provide the same level of protection as the hospital network.

Even so, hospital personnel should collect fax messages immediately after they are received to ensure no one intercept them and the confidentiality of the content is secured.

Secure MFD telecommunications

An MFD can act as a bridge between a network and a telephone system when connected to both, so the digital telephone system must function at the same sensitivity as the network and have controls that are similar to other devices present on the hospital network.

Video Conferencing Applications

Microphones and webcams

Microphones and webcams attached to workstations can present a security risk as they can be activated via malicious applications unintentionally installed on the workstations. As such, microphones and webcams can operate as remote listening/recording devices.

Video conferencing

Video conferencing and IP telephony infrastructure used by hospital personnel are susceptible to various cyber threats such as eavesdropping, man-in-the-middle attacks, call spoofing, and DOS attacks. To reduce these security risks, video and audio data is protected using Transport Layer Security and Encrypted protocols.

Additionally, to reduce the likelihood of an unauthorised party accessing video conference or IP telephony infrastructure, it is important to automatically block unauthenticated or unauthorised devices.

Approved video communication applications

The CISO and cybersecurity department are responsible for evaluating and curating a list of communication applications for use by hospital personnel. These applications meet the security and encryption requirements and are well supported by their developers with regular updates. While applications such as Zoom, Skype Video, and FaceTime may be approved for limited use, such as for outpatient calls and meetings, they still present risks to the system. Staff must be trained on their proper usage, avoid transmitting highly sensitive data, and understand the laws that govern the transmission and storage of confidential data such as patient records.

SOCIAL MEDIA USE, GUIDELINES

The careless sharing of sensitive data on social media can be illegal, and result in breaches of privacy laws and intellectual property law compliancy. Social media guidelines must be a strong component in the cyber awareness training of all staff, and actively monitored.

Official accounts representing the interests of the hospital brand also abide by these guidelines, including third-party representation.

Compliancy rules

Guidelines on how to comply with privacy and confidentiality legislation, copyright laws, intellectual property laws, and ethical social contract rules. This includes strongly worded instructions on how to handle patient information and healthcare data.

A plan of action during a PR crisis

A crisis management plan should be prepared by the PR department, that covers an emergency list of important individuals designated in dealing with a social medial emergency; the Chief Information Officer (CIO), social media team, legal department, and CEO. Guidelines for determining the scope and impact of the crisis, and response plans for mitigation and clean up should be formulated.

General social media roles, responsibilities

Social media roles and their scope of use need to be established, including their responsibilities. Factors defined are frequency of posting, engagement rules, customer service scope, advertising, PR strategies, security aspects, content creation, and general posting rules.

Non-discriminatory, human-rights purveyor

Rules for posting are to be set, governed by social contracts of the day, culture set by the hospital management, and legislations of the sate the hospital operates in. This contains provisions that prohibit racism, sexism, bigotry, and discrimination against political, religious, medical, cultural choices, and sexual orientation. As hospitals are a place of healing, judgement of an individual’s actions, or lack of actions, is not permissible.

Staff use of personnel social media accounts

Personnel are instructed to keep their own personal information posted on social media to bare minimum or in private. Emphasis is placed on training staff to understand the types of information they post that may pose a risk to the hospital, such as information that facilitates social engineering attacks, or offers insight into the hospital’s security/network deployment or organisational structure. Posting information on staff activities or jobs and their responsibilities is strictly forbidden, along with publicly posting solacious and malicious information.

Staff are contractually obliged to positively reflect the brand image of the hospital and its mission statement and are encouraged to respect the hospital’s non-discrimination culture, and the human rights of all peoples.

Finally, it goes without saying that staff must always adhere to patient/doctor privileges and privacy laws.

CYBERSECURITY AWARENESS TRAINING GUIDELINES

This section provides recommendations and advice on the cybersecurity awareness training of all hospital staff and third-party contractors, such as topics of discussion and importance, how often retraining occurs, policy enforcement and consequences, level of training defined by staff roles, how the training is undertaken.

The scope of this cybersecurity awareness training is limited to advice and recommendations only. Each organisation must hire adequate expert input to properly design the curriculum and subject matter that is appropriate. The hospital leverages the expertise of the hospital's Chief Executive Intelligence Officer (CISO) or similar role, to work with all the relevant departments required to formulate and design the most appropriate cybersecurity awareness training material.

Cybersecurity awareness program

The CISO is responsible for overseeing the development of the awareness training program, ensuring that all hospital staff are actively participating in the cyber protection and defence of the hospital's systems. External expertise can be employed, along with organisations that provide specialised cybersecurity training. The CISO's role is to liaise between all parties involved and submit the training curriculum to the hospital's administration, legal department, and HR department for review and approval.

Preparing cybersecurity training instructors

The CISO oversees the hospital's cybersecurity taskforce, organising the plans and strategies to train and maintain the training of the cybersecurity personnel. As such, the CISO delegates the relevant training tasks to the cybersecurity and departmental heads that are required to handle the training of all hospital staff. Adequate authority is bestowed on managers, and the resources required to perform the training are provided.

Role-Based Training

There is a myriad of roles and responsibilities undertaken within the hospital, in carrying out its duty of care for the patients and the stakeholders. No staff is exclusive and above the need for cyber awareness training, and this even includes the CEOs and Board Members; there are serious legal and financial ramifications to breaches of patient privacy and data integrity laws.

Naturally, while a degree of tact is required to handle the boardroom's cyber training compliancy, most staff will readily comply.

Training intensity is broken down into role-based needs:

1. The most intensive training, with most frequent retraining, is undertaken by cybersecurity personnel, network engineers, and system administrators: job roles that contribute to the implementation and maintenance of security within the hospital network and information systems.
2. Normal training level, for all job roles that regularly require access to the network and information systems, to carry out their duty. Retraining is less frequent.

3. Minimal training, for third-party and external contractor job roles. Hospitals are a busy place, and many third-party or contractor personnel are transient and short stayed. The most important information and policies related to their tasks are provided and signed for before they are allowed to engage in their tasks. People in this role are severely restricted in their system access, and physically limited to specific locations.

Frequency, Delivery Methods

New employee training

The most intense training occurs when new staff are taken on board and is a condition of their terms of hire. New employee cyber awareness training must be completed at their induction before access to any secure systems can take place. They are to be given a user profile, with restricted access, and required to choose their password according to the password policy rules.

Retraining Frequency

Whenever an important update is made to policies (and subsequently training material) that is critical in maintaining the cyber integrity of the hospital, the new policies and/or training must be refreshed for all related roles.

Retraining frequency is recommended:

I. Once a year for all staff minimum, half a day of paid on-premises training, through the supplied training application. Simple tests are undertaken to ensure all staff understand the potential impact of risky activities.

II. Smaller quarterly updates for staff to read and digitally sign, including changes to policies and hospital rules.

III. Whenever critical events occur, such as zero-day exploits that must be communicated, or when an actual serious cyber incident has occurred, and corrective actions are issued.

Cyber Training Topics

The CISO is responsible for arranging with the relevant experts the cyber training curriculum. This will be defined by the hospital’s threat landscape, business goals, mission statement, laws, and ethical responsibilities.

Here are several recommended training topics for cyber awareness training:

- Password rules and policy
- Legal responsibilities of using healthcare/patient data
- Responsibility of company data
- Document management, transmission, storage
- Software use / unauthorized software
- Internet access and usage
- Emails, confidentiality, privacy laws
- Email attachments, viruses
- Malware and virus concepts

- Social engineering and phishing attacks
- Social media usage and policy
- Posting working information online
- Sending/receiving work files via online services
- Use of third-party communication apps
- Telephone and fax usage
- Work mobile devices usage, on/off premises
- BYOD device rules
- Physical access rules
- Hardware and ICT equipment usage
- Media usage, intellectual property
- Database usage and security concepts
- Basic concepts of network and information security

Passive Cyber Training Signage

It is recommended that constant reminders and critical cyber information be presented to hospital personnel in the form of signs on the wall, stickers printed on equipment, reminders in meetings, and banners located at the login portion of all services used within the hospital.

The ACSC recommends the following logon banner reminders cover the following topics (cyber.gov.au 2022):

- the sensitivity or classification of the system
- access to the system being restricted to authorised users
- acceptable usage and security policies for the system
- an agreement to abide by acceptable usage and security policies for the system
- legal ramifications of violating acceptable usage and security policies for the system
- details of any monitoring activities for the system.

RISK ASSESSMENT OUTLINE

The risks factors for the hospital network are defined, identified, and analysed using the official NIST recommended methodology (Guide for conducting risk assessments, 2012).

A risk assessment was planned and executed, and the resulting report was communicated with the hospital administration, network engineers, and security specialists who are involved in the planning, implementing, and managing of the hospital network. This risk assessment is an important aid in implementing risk prevention for the network design, security design, and security policy formulation, of the hospital network and information systems.

For the full report, view the Risk Assessment Report (Risk-Assessment-Report.docx).

Main Threat Events

Research was conducted into common vulnerabilities and risks associated with healthcare networks and information systems, successfully identifying the following threat events. These are the main threat events to be considered in the cybersecurity planning and management for the hospital.

Table 1: Potential Network/Information System Threat Events

TYPE	IDENTIFIED THREAT EVENTS
Adversarial	**Hacking, data theft, data loss risks.** Electronic health records, or EHRs, contain sensitive and private information pertaining to patients' medical data, and are a prime target for threat actors and data thieves.
Adversarial, Personnel	**Ransomware and phishing risks**. In the last decade, hospitals have become one of the main targets for phishing and ransomware attacks. Ransomware has a high impact risk potential, as blackmailers can often cripple systems and demand huge payouts.
Adversarial, Personnel	**Reliance on medical IoTs, WIFI and remote access risks.** Through wireless networks (WIFI), Bluetooth, and remote connectivity; hospitals and healthcare systems make use of many medical devices that all transmit and store sensitive data, in the cloud or elsewhere.
Structural	**Aging network infrastructure, software, and 3rd party reliance, risks**: As information technology and medical treatment innovations rapidly evolve, this results in an increasing complexity and interdependency of aging infrastructure and newer patched networks with a myriad of new and old software.
Personnel	**Loss of compliance risks.** Many countries have strict regulatory laws that govern patient privacy and confidentiality, and how their data is collected and stored. For example, the HIPAA was passed in 1996 in the USA, with The Privacy Act 1988 as the Australian counterpart.
Personnel	**Lack of cybersecurity awareness risks.** Hospitals and healthcare facilities operate with hundreds or even thousands of personnel, filling a vast range of roles and duties that often require use of restricted systems and access to sensitive information.

TYPE	IDENTIFIED THREAT EVENTS
Environmental	**Natural disasters and failures of critical systems:** As already noted, the operational readiness of critical systems is of the highest performance, as they are required to service patients with, often in a lifesaving capacity.

Highest Potential Risks

Here is a tabled list of the highest risks (Table 2), which have the highest potential for negative impact, and highest potential of occurring; that have a critical need to be mitigated and monitored during the planning, design, implementation, and management of the hospital network and systems.

Table 2: Risks that require the highest level of attention

Risk Threat	Impact Factors	Impact
Ransomware (*Adversarial*)	Malware encrypts data, potential data loss or corruption, loss of system services availability, or financial costs due to loss of productivity and blackmail.	High
System Penetration Attacks, Hacking. (*Adversarial*)	Hospital network, WIFI, information systems, databases, patient records, online services, staff workstations, and sensitive medical equipment at risk of compromise or theft of data.	High
Hospital staff introducing risk events. (*Personnel*)	Data suggests that humans introduce most risks from within a secure system. Poor behaviour, insecure activities and operational mistakes that introduce adversarial events such as malware, viruses, and system intrusion. Or activities that increase structural risks.	High
Data loss, or database fail (*Structural*)	Server or software component failure leading to partial loss of databases serving or storing critical information. Information systems and services dependent on the data may fail to operate correctly.	High
Network hardware failure, WIFI failure (*Structural*)	Hardware component failure leading to partial loss of network infrastructure or information systems. Also resulting in medical IoT device loss of connectivity, and operability.	High
Loss of data compliance (*Personnel*)	The Privacy Act 1998 dictates laws governing the handling of confidential information and data. Large breaches in confidentiality laws resulting in litigation and fines.	High

SECURITY POLICY SECTION

This section gives recommendations and advice on policies: a comprehensive list, how often they should be reviewed, how they are enforced, and actions to be taken in the event of policy failure.

Policy Management

In the business of policy management, it is generally recognised there are four main processes that make up the policies life cycle:

1. **Writing and creating organisational-specific policies.** This involves a process of discovery. For the hospital a strong focus was placed on the threat events and risk factors specific to large healthcare organisations. NIST policy templates were used as a foundational structure.
2. **Communicating the policies.** Hospital administration, network engineers, system administrators, and the cybersecurity personnel, are the primary disseminators of such policies. All personal and third-party contractors are required to read and agree to all policies that govern their area of duty.
3. **Managing and enforcing the policies.** Consistent management and enforcement of policies plays a critical role in the actual usefulness of policies and their rules. For the hospital, the Chief Information Security Officer (CISO) oversees the entire life cycle of all policies and is charged with their management and enforcement. The CISO works with the hospital board, administration, HR, legal department, IT/cybersecurity department, and external partners and vendors. Accuracy and compliancy with laws and legislation that govern healthcare services are especially enforced.
4. **Maintaining policies.** The hospital's policies are subject to regular reviews, updating any changes to the hospital's rules in general, institutional rules, compliancy with changes in legislation and laws, and proactive improvements to the cyber defence and protection measures utilised. Advice from the hospital's legal department should be sought, as to the frequency of policy update that govern legal compliancy. All other policies should be reviewed on a quarterly basis.

   Policy changes must also be tracked and dated, this is important legally, and administratively. When a policy is updated, the CISO and all departments must re-communicate the policy with all hospital staff. A process must be in place to account for this, such as using policy management software that records staff compliancy.

   The policy life-cycle workflow process must also be annually reviewed, to identify new weaknesses, and also new processes made available that can improve the policy management.

Policy Enforcement and Consequence

Any employee, contractor, or third-party service provider who violates security policies may be subject to disciplinary action, termination of employment or contract, and possible litigation in cases where the breach results in financial impact. The legal department, hospital board, and administration are to aid the CISO who is charged with producing comprehensive review processes and enforcement procedures, in the case of suspected or reported policy breaches.

Policy Directory

Several policies were produced specifically (Table 3) to govern the unique risk events of the hospital network, information systems, databases, communications, physical hardware and environment, personnel and staff, and other third-party factors.

Table 3: Policy Directory

Policy	Purpose and Use
Password-Policy-and-Guidance.docx	To provide a set of rules and guidelines to enable staff to create strong passwords and to keep those passwords safe from exposure to any other parties.
Policy-Acceptable-Use.docx	To outline the acceptable use of computer equipment at the Hospital. These rules are in place to protect the employee, the Hospital, and the patients.
Policy-Anti-Virus-Policy.docx	To provide guidelines to help prevent the infection of hospital resources with viruses or malware.
Policy-Data-Breach-Response.docx	To define the roles, responsibilities, and processes to be followed in response to an identified or suspected breach of confidential or sensitive data, including reporting the breach to the appropriate authorities and those affected.
Policy-Email.docx	To ensure the proper use of the hospital's email system and make users aware of what the hospital deems as acceptable and unacceptable use of its email system. Misuse of email can pose many legal, privacy and security risks.
Policy-Encryption-Standards.docx	To provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively, to ensure that laws governing the accessing and use of personal health records are adhered to.
Policy-Software-Installation.docx	To outline the requirements around installation and use of software on Hospital computing devices, to minimize the risk of loss of program functionality, the exposure of sensitive information, and reduce the risk of introducing malware.
Policy-WiFi-Device-Access-Standards.docx	To specify the technical requirements that wireless infrastructure devices must satisfy to connect to a hospital network. Only those wireless infrastructure devices that meet the requirements specified by the IT Department are approved for connectivity to a hospital network.
Policy-WorkStation-Guidlines.docx	This policy document aims to provide practical guidance for hospital staff when using hospital information systems, such as rules when accessing and transmitting confidential and sensitive patient information.

REFERENCES

Australian Government (2014). Privacy Act 1988. [online] Legislation.gov.au. Available at: https://www.legislation.gov.au/details/c2014c00076.

Guide for conducting risk assessments. (2012). [online] doi:10.6028/nist.sp.800-30r1.

Microsoft (n.d.). Why a risk-based approach to cybersecurity is the right business choice | Microsoft Australia. [online] Available at: https://www.microsoft.com/en-au/business/topic/security/managing-cyber-risk/why-a-risk-based-approach-to-cybersecurity-is-the-right-choice/.

NIST (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. [online] csrc.nist.gov. Available at: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

www.cyber.gov.au. (2022). Australian Government Information Security Manual (ISM) | Cyber.gov.au. [online] Available at: https://www.cyber.gov.au/acsc/view-all-content/ism.