HSU
NSW•ACT•QLD

IT Security Policy

Document Information

Document Status	
Version Number:	2.0
Last Update:	30 November 2023
Document Title:	IT Security Policy

Version:	Issue Date:	Comments	Approved By:
1.0	14 July 2019	Initial policy implementation	Union Council - 14/2019
2.0	30 November 2023	Updated IT Security Policy	Union Council – 75/2023

This policy is a living document and can be updated as determined by those responsible for updates and revisions. Ad hoc and scheduled reviews should also take place to reflect the changing requirements within the Health Services Union.

All requests for changes can be submitted to the policy owner, who will discuss change requests with the relevant stakeholders and accept or reject the request. Following approval by Union Council, the change(s) will be incorporated into this policy.

Confidentiality

You should carefully review the following confidentiality condition prior to reading or using this document.

This document contains confidential information of which you may not directly or indirectly use, disclose, or publish or permit its use, disclosure or publication without the express written permission of Health Services Union.

Reading or using this document indicates your acceptance of this confidentiality condition. If you do not agree with these terms and conditions, you should promptly return the document to Health Services Union.

This confidentiality condition forms a binding agreement between you and Health Services Union.

Table of Contents

IT Security Policy

1. Purpose

The Information Technology Security Policy outlines the organisation's requirements to protect *Health Services Union* information in different stages of processing, transmission, or storage. This forms part of the organisation's suite of policies aiming to protect the confidentiality, integrity and availability of all *Health Services Union* and our clients' information, especially classified information, such as payment card information.

The intention of this policy is to provide guidelines, for employees to apply personal judgment in their use of *Health Services Union*'s resources to protect its technology, infrastructure, and people to reduce the exposure of risks to information. Mishandling of information could occur intentionally or unintentionally, resulting in incidents such as data breaches and impact the integrity of *Health Services Union* and its customers' information, as well as our corporate reputation.

This policy is also designed to adhere to Payment Card Industry (PCI) Data Security Standard (DSS) v3.2 requirements. *Health Services Union* understands that some clients are required to comply with PCI DSS due to transmitting, storing, or processing payment card information (e.g., credit card details). Refer to the Compliance section for further information.

2. Scope

This policy applies to all officers and staff, including full time and part time employees, contractors, consultants, and other workers at the organisation's offices and customer service sites, including all personnel affiliated with third parties.

This Policy outlines the criteria for easily classifying and protecting *Health Services Union* 's and its members' information resources, particularly with regard to the following types of information:

- Member information
- Budgets and business plans
- Employees' personal information

The level and type of access for employees may vary depending on the organisation's requirements.

3. Accountability

The following personnel have designated responsibilities to information security management regarding the requirements in this policy:

Role Title	Accountability
Chief Financial Officer (CFO)	Ensure all *Health Services Union* information is securely maintained, and compliance requirements are adhered.
IT Manager	Ensure all systems and monitoring takes place as needed.
Information Technology (IT) Administrator	Ensure all technical systems are adequately controlled in line with this policy and users are only provisioned access and use as per their role requirements.
Managed Services Provider	Provide 2nd tier support and monitoring of servers and all IT related services. Supplying additional support in house when IT is under resources due to leave.
Human Resources Manager(s)	Ensure all users adhere to this policy and non- compliance or deviation from this policy is managed.
End User(s)	Follow this policy and ask for further clarification if required.
Third Party (ies)	Be aware of this policy and adhere to it if working on *Health Services Union* premises and using *Health Services Union* 's IT resources.
Information Asset Owner	The *Health Services Union* may choose to allocate information owners who are responsible for overseeing that information is appropriately classified, accessed and managed.

4. Management Roles and Responsibilities

The IT Manager is responsible for aiding the IT Administrator in promulgating a set of industry standard compliant security technical standards, including the following:

- Network design, router, and firewall configuration standards.
- Server build, hardening and patching standards.
- The establishment of sound user verification and identification policies, ensuring that all actions taken can be traced back to individuals, and that opportunities for unauthorised access to information are minimised.
- The establishment of security monitoring practices, including network intrusion detection, prevention, incident logging, file integrity monitoring and Security Event correlation alerting.
- Methods and practices for the secure storage and transmission of private and confidential data.
- Establishing a program of risk review and mitigation, including internal and external testing of network and systems vulnerabilities.
- Establishing and maintaining a sound change management system.
- Establishing and maintaining an incident response process, which addresses legal, contractual, and

technical responses to any incident which impacts on the Confidentiality, Availability, or Integrity of *Health Services Union* 's information assets.

- A set of processes for managing service providers and vendors in their interaction with *Health Services Union* 's information assets.

5. PCI Roles and Responsibilities

The following information security responsibilities must be specifically and formally assigned:

Responsibility	Individual or Team Assigned
Overseeing and ensuring *HEALTH SERVICES UNION* maintains a PCI Compliance program which is audited and complied with on an annual basis.	CFO
Ensure an effective security awareness program is in place.	IT Services Division
Ensuring *Health Services Union's* management is adequately informed of their responsibilities with regards to protection of Cardholder Data.	CFO / IT Manager
Ensuring all new environments are implemented in a manner that complies with the PCI DSS. *Health Services Union*	IT Services Division/ Managed Service Provider
Monitor and analyse security alerts and information and distribute to appropriate personnel.	IT Administrator / Managed Service Provider
Management of network components	IT Administrator / Managed Service Provider
Establishing, documenting, and distributing security policies and procedures	CFO / IT Services Division/ HR
Administration of user accounts, including additions, deletions, modifications, and authentication management	IT Services Division
Monitor and control all access to data. Implementing access controls. (for IT Support and CRM support)	IT Services Division

6. Protection of Information

The Health Services Union must have a formal approach to identify and protect the Confidentiality, Integrity, and Availability of all its information assets. This will ensure safeguard of its information and that of its clients, the continuity of its operations, minimise the impact, should information security incident occur.

- Implement Information Security framework or strategy based on industry best practices (ISO 27001/2) to ensure secure management of all information across the organisation.
- Ensure that its information security practices are enforceable by all employees by understanding the information asset type, classification, and protective measures.
- *Do not* store PAN details under any circumstances on any system, including data system or hard copy. Any evidence of CHD must be destroyed. If PAN is required to be stored, then appropriate encryption methods must be used in line with PCI DSS requirements.
- Implement suitable controls, which consist of people, policies, procedure, standards, guidelines, and technologies (hardware and software) to mitigate any exposure to its own or clients' information.
- *Health Services Union shall* measure the effectiveness of its controls through risk assessment (refer to *Health Services Union* 's Information Risk Assessment procedure), vulnerability management, security audits and compliance checks.
- Retention period for assets and data must be determined based on business and regulatory requirements. These should not be retained longer than required. There are associated policies and guidelines for these topics.
- For PCI DSS compliance, event logs from anti-virus software should be kept for a year and at least three months is available for immediate analysis.
- Data classification information shall be documented, reviewed, approved, and disseminated to all staff. Policy shall include Labelling, Retention, Media Handling and Destruction process and procedures. (refer to policies in separate document).

7. IT Security Policy

7.1 Staff Induction and Training

It is necessary to have formal procedures in place so that access to systems by new staff is carried out in a secure and consistent manner. Procedures for authorising, establishing, and modifying access privileges must be followed, implemented, and maintained. This includes requesting, authorizing, and allowing access in an emergency:

- All employees must have successfully passed background checks prior to commencing employment, including, where appropriate, credit and criminal history checks.
- All employees must provide written acknowledge that they have read and understood the Information Security policy and relevant procedures. Requiring an acknowledgement by personnel in writing or electronically helps ensure that they have read and understood the security policies/procedures, and that they have made and will continue to make a commitment to comply with these policies.
- Formal authorisation forms must be completed and signed by the new staff members and their Department Manager. These forms must also be authorised by the IT Services Division, before access will be provided.
- The Human Resources Department will ensure that new staff are given appropriate Information Security education and awareness training prior to access being granted to systems and information.
- Employees must undergo security awareness training including cardholder data security on commencement at *Health Services Union* and at least annually. It may be computer based, team meeting, quiz etc. This must specifically cover compliance requirements such as PCI DSS.

Appropriate training will also be provided annually to staff with security breach responsibilities. All personnel must formally acknowledge that they have read and understood the security policy and procedures at least annually. Attendance of training and awareness programs should be maintainedby HR team to ensure refresher training is undertaken on an annual basis.

- Staff changing functions or requiring changes to their access privileges must submit a new staff access request to IT Services Division by their direct line managerc

7.2 Access Controls

- Strict Policy on General Access Controls must be followed as below:
  - Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:
    - Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
    - Assign access based on individual personnel's job classification and function.
    - Require documented approval by authorized parties specifying required privileges.
  - Restrict access based on a user's need to know, and control is set to "deny all" unless specifically allowed. This access control system must include the following:
    - Coverage of all system components
    - Assignment of privileges to individuals based on job classification and function
    - Default "deny-all" setting

7.3 Terminating Staff

- Terminated staff will have authorisation and access privileges revoked promptly.
- Application owners are responsible for reviewing the Staff Movements notification generated by the exiting staff member's Department Manager. IT will be responsible for removing access by relevant users to the systems.
- IT will be notified immediately of the termination of a user deemed to be a security risk. Their access will be revoked immediately.

7.4 Asset Database and Registers

7.4.1 Software List

- Only software intended, approved, and correctly licensed for *Health Services Union's* business goals may be installed or used on any *Health Services Union's* computing device.
- A List or a Register of Approved Products and correctly licensed Software permitted for use within *Health Services Union* must be maintained, periodically reviewed, and updated. Responsibility must be explicitly assigned.
- Owners must at a minimum:
  - Determine the sensitivity and/or criticality of the product/software/Operating System under their control
  - Check that the appropriate protection measures are in place
  - Authorise and periodically review access rights to their software and applications
  - Facilitate the resolution of security-related audit issues
  - Periodically review the risk classifications of application software under their control
  - Maintain an inventory of software under their control which should contain personnel information authorised to use the devices.
- List of software running on the server shall include operating system, programs, and services running on the server.

7.4.2 Hardware List

- IT will maintain an accurate and up to date register of all *Health Services Union* IT equipment. This includes listing of all routers and firewalls, along with the access controls provided by each device.

- Remote Access and Remote-Control solutions used to access systems must be on the approved security solution list.
- Only *Health Services Union* IT Services Division staff are authorised to configure, set up and build hardware within the *Health Services Union* business environment consequently only they are authorised to install/un- install software within the *Health Services Union* IT standard operating environment and remote organisers have rights to install approved application they need.

7.5 Hardware & Asset Tags

- All mobile phones, computers, laptops, and desktops will be marked with a unique Health Services Union asset tag.
- All Health Services Union's computer and communications equipment must have a unique identifier ie serial number / asset tag to it such that physical inventories can be efficiently and regularly conducted.
- Labelling should include information such as owner, contact information, and purpose which is included in the Asset register with IT.

7.6 Virus Controls

- Current and up to date anti-virus software must be installed and used on all computers. All anti-virus software must be active regularly updated and capable of generating audit logs.
- Approved malicious code detection software must be installed and utilised: on all vulnerable devices, including but not limited to personal computers, mobile phones, and PDAs at e-mail gateways and messaging servers.
- *Health Services Union* systems must have Anti-Virus, Anti-Spyware and Host Intrusion Prevention modules installed, where required, to provide coverage for different threat vectors.
- Malicious code detection software and signature files must be:
  - maintained at latest vendor levels,
  - configured to monitor and intercept malicious code in real time,
  - configured using the established global anti-virus software configuration
  - For any systems in the PCI DSS environment the Antivirus event logs should be kept for a year with 3 months available online for analysis.

7.7 Firewall Configuration

PCI DSS requires that Firewall and configuration standards must be established and implemented to protect cardholder data. The *Health Services Union's* Firewall configuration standards below must be implemented and followed:

- All network connections and changes to the firewall and router configurations must be formally submitted via proper change process, tested reviewed and approved by authorised personnel. Changes to configuration settings and rules for routers, switches, IDS/IPS and firewall devices shall be confirmed as meeting the business and security objectives before releasing the change into Production status.
- Network diagram showing cardholder data flows over the network must document all connections to cardholder data, including any wireless networks and must be maintained, reviewed, and kept current.
- Firewall configuration standards must require that a firewall be implemented and installed:
  - At each Internet connection.
  - Description of groups, roles, and responsibilities for management of network components must be updated and kept current
  - Use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure must be in place and business justification for use of those services and protocols is provided.
  - Routers, switches, firewalls, and IPS/IDS capabilities shall be employed to enable network segregation,

traffic flow control and auditing of network events.

  - Firewalls and appropriate network address allocations shall be used to facilitate security zones and need to know access according to industry standards and PCI DSS requirements.
  - Firewall and router configurations must restrict connections between untrusted networks and any system components in the cardholder data environment.
  - Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic
  - Perimeter firewalls installed between any wireless networks and systems that store cardholder data, deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. Secure and synchronize router configuration files.
  - Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. Direct access between publicly accessible environments and the cardholder environment must be prohibited. This applies to both inbound and outbound traffic.
  - Traffic must not be allowed to cross the firewall unless explicitly permitted. Filtering of traffic to control and restrict access across the perimeter between the corporate intranet and the public Internet or other untrusted networks must be utilized. This filtering includes, but is not limited to, destination and source IP addresses, ports, applications, and protocols. Network Address Translation (NAT) NAT technologies must be used to mask internal IP addresses and only display an external IP address.
  - IP addresses for the private intranet must not be propagated into any untrusted network unless necessary to ensure connectivity and availability
  - Settings and rules that are identified as no longer meeting *Health Services Union* 's business objectives shall be revised, deleted, or disabled.
  - After configuration of routers and firewalls, the running and start-up configurations must be synchronised, and checksums compared to ensure that following a re-boot the running configuration is restored as approved. Backup copies of configuration settings and rules for IDS/IPS and firewall devices shall be maintained.
  - Configuration settings and rules for routers, switches, IDS/IPS and firewall devices shall be reviewed every six month.
  - The minimum requirements for configuration settings and rules for routers, switches, IDS/IPS and firewall devices shall be documented, including permitted protocols, services, source, and destination addresses etc. shall be reviewed and updated at least annually or when significant changes occur.
  - Listing of all routers, along with the access controls provided by each router, must be maintained.

7.8 Wireless Environment Controls

- Firmware of wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks and updated from time to time as recommended by the equipment vendor to retain a secure status. Communications used to remotely manage security functions or devices that provide security controls must be encrypted and authenticated before transmission.
- All security-related vendor defaults for wireless devices must be changed prior to use.
- Vendor supplied default passwords and PINs must be changed prior to implementation into a production environment
- All electronic connections to or from third parties must undergo pre-production connection testing and security assessment. Production use must not occur unless acceptable test results have been obtained.
- The community strings for SNMP must be changed from the vendor defaults.
- Documented inventory records of authorised wireless access points must be maintained, and a business justification is documented for all authorized wireless access points.
- Scanning either before the system is implemented for its intended purpose as a part of the infrastructure or whenever a potential intrusion is identified must be performed and reviewed at least twice a year on all networks, sub-networks and individual machines that are connected to the enterprise.
- Policy must include notification requirement to alert appropriate personnel if automated monitoring is employed for the detection of unauthorised wireless access points.

7.9 Remote Access

- Remote Access and Remote-Control solutions used to access systems must be on the approved security solution list.
- Only approved security devices, such as firewalls, VPN, IDS and IPS, are authorised to be implemented within the *Health Services Union* 's environment. All such devices must be configured in a manner to protect against the circumvention, subversion, or undermining of the required level of security in accordance with industry accepted standards.
- Requests for access to the network through remote access services must be approved by an appropriate level of management
- The ability to copy, move, and store cardholder data onto local hard drives and removable electronic media must be prohibited via remote access technologies.
- Usage policies and proper use of critical technologies shall include remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.

7.9.1 Third Party Remote Access

- All electronic connections to or from third parties must undergo pre-production connection testing and security assessment. Production use must not occur unless acceptable test results have been obtained.
- Remote access for third parties must only be enabled during the time needed and deactivated immediately after use.
- Remote access sessions must be automatically disconnected after a specific period of inactivity.
- IDs used by vendors to access, support, or maintain system components via remote access will be managed as follows:
  - Monitored when in use.
  - Repeated access attempts will be limited by locking out the user ID after not more than six attempts.
  - Lockout duration will be set to a minimum of 45 minutes or until an administrator enables the user ID.
  - Remote access will be deactivated or removed from the access list for users that has been terminated.

7.10 System Configuration

All policies listed below are to comply with PCI DSS requirement 2.2:

- Develop configuration standards for all system components and ensure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards
- All *Health Services Union* computers, devices and applications shall be configured and hardened to meet the intent of this policy and industry standards.
- A Configuration Standard policy should define how system components are configured to the function that is required. Document should show services and port enabled / disabled, list what accounts and password types should be created; or can be very detailed and list step by step how to setup a system component. However, the document should be in line with industry accepted hardening standards and should include instructions for testing that the required hardening has been achieved.
- No changes to any configuration setting on computers, devices and applications are permitted without first having been approved according to *Health Services Union's* Change Management Procedures. This includes workstations, laptops and similar.
- Approved configurations must be followed to configure remote access services. All *Health Services Union* computers, devices and applications shall be configured and hardened to meet the intent of this policy and industry standards.
- Application or system services not being used for a defined business purpose must be disabled, including any part of the operating system that is unnecessary to the business purpose of the system. (E.g. daemons, "insecure" protocols). If ports, services, daemons, or protocols that are considered "insecure" are being used they need to be justified and security features need to be documented. Additionally, an evidence of security features and controls implemented to mitigate the associated risks

must be provided.)

- That common security parameters settings are included and are set appropriately.

7.11 Server Security

This policy is to set out required minimal security configuration for all server equipment connecting to a production network or used in a production capacity at or on behalf of the *Health Services Union.*

All internal servers deployed are owned by the *Health Services Union* IT Department / Managed Service Provider who are responsible for system administration. Approved server configuration guides which comply with general industry accepted standards (CIS, NIST) must be established and maintained by each operational team, based on business needs and approved by *Health Services Union* IT. The IT teams will monitor configuration compliance and implement an exception policy tailored to their environment. Each IT team must adhere to the IT Department process for changing the configuration guides, which includes review and approval by IT Management.

At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact.
- Hardware and Operating System/Version.
- Main functions and applications, if applicable.
- Information in the corporate enterprise management system must be kept up-to-date.
- List of software running on the server including operating system, programs, and services running on the server.
- Configuration information about how the server is configured including:
  - Event logging settings
  - A comprehensive list of services that are running.
  - Configuration of any security lockdown tool or setting
  - Account settings
  - Configuration and settings of software running on the server.
- Types of data stored on the server.
- The owners of the data stored on the server.
- The sensitivity of data stored on the server.
- Data on the server that should be backed up along with its location.
- Users or groups with access to data stored on the server.
- Administrators on the server with a list of rights of each administrator.
- The authentication process and protocols used for authentication for users of data on the server.
- The authentication process and protocols used for authentication for administrators on the server.
- Data encryption requirements.
- Authentication encryption requirements.
- List of users accessing data from remote locations and type of media they access data through such as internet or private network.
- List of administrators administrating the server from remote locations and type of media they access the server through such as internet or private network.
- Intrusion detection and prevention method used on the server.
- Latest patch to operating system and each service running.
- Groups or individuals with physical access to the area the server is in and the type of access, such as key or card access.
- Emergency recovery disk and date of last update.

- Disaster recovery plan and location of backup data.
- Configuration changes for production servers must follow the appropriate change management procedures.
    - Operating System configuration should be in accordance with approved IT guidelines.
    - Services and applications that will not be used must be disabled where practical.
    - Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

7.12 Patch Management

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Security patches or mitigation measures must only be communicated and delivered through approved *Health Services Union* processes. Patches or mitigation measures must be reviewed for impact and applicability to the environment and, if appropriate, applied using standard change control procedures. High severity security patches must be installed within 1 month of release.
- Maintain current knowledge of available patches by keeping up with vendor releases and updates.
- Decide what patches are appropriate for particular systems by identifying and assessing the impact of system vulnerabilities and likelihood of exploits eventuating.
- Ensure that patches are installed properly to mitigate system vulnerabilities by testing the patches on test systems prior to installation.
- Verify systems after the installation of patches to ensure successful patch implementation and the vulnerability is no longer present.
- Document all associated procedures and ensuring the procedural steps and roles and responsibilities are kept current.
- Patches are to be tested and evaluated for negative system impact and risk. The vulnerability mitigated by the patch will be evaluated against the impact to business, such as loss of business functionality or operations, other potential vulnerabilities introduced by applying the patch, and availability of system resources.

7.13 Logging and Monitoring Controls

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.

PCI DSS requirement 10 lists the following which must be followed:

- Implement audit trails to link all access to system components to each individual user.
- Implement automated audit trails for all system components to reconstruct the following events:
    - All actions taken by any individual with root or administrative privileges
    - Access to all audit trails.
    - Invalid logical access attempts.
- Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.
- Initialization, stopping, or pausing of the audit logs.
- Creation and deletion of system-level objects.
- Record at least the following audit trail entries for all system components for each event:

- Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

  Note: One example of time synchronization technology is Network Time Protocol (NTP)." Critical systems have the correct and consistent time

  - Time data is protected.
  - Time settings are received from industry-accepted time sources.
  - Secure audit trails so they cannot be altered.
  - Limit viewing of audit trails to those with a job-related need.
  - Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
  - Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.
  - Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
  - Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement. "
  - Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
  - Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
  - Follow up exceptions and anomalies identified during the review process.
  - Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).
  - Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.

8. Vulnerability Management

A vulnerability scan is an automated tool run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals.

There are 2 types of vulnerability scanning required for PCI DSS:

- External month vulnerability scanning, which must be performed by an ASV on Firewall
- Internal and external scanning as needed once a year. Once these weaknesses are identified, the entity corrects them and repeats the scan until all vulnerabilities have been corrected.

Identifying and addressing vulnerabilities in a timely manner reduces the likelihood of a vulnerability being exploited and potential compromise of a system component or cardholder data.

The *Health Services Union* shall run internal and external network vulnerability scans at least yearly.

9. Business Continuity and Disaster Recovery

- The organisation must have a Business Continuity (BCP) and Disaster Recovery (DR) practices in place to ensure its services are uninterrupted and continuously available.
  - Ensure that its client services are uninterrupted, and the availability of services outlined in client contracts is met.
  - Adequate BCP and DR plans should be documented and tested on an annual basis when required.
  - BCP and DR plans of its own network environment must exist and ensure employees are able to perform their business duties efficiently.

10. Risk Assessment

- Ensure all non-compliances, deviations, exposures and gaps are identified and managed as risks.
- Identify and assess risks as per Risk Assessment procedure. A risk assessment must occur least annually to identify threats and vulnerabilities.
- Ensure high and extreme risks are treated as a priority.
- Ensure where feasible, compensating controls are implemented.

Below is the standard Risk Management Cycle as described in ISO 31000:2009 and ISO 27001:2011. This encompasses many phases which aim to provide consistent assessments with comparable and repeatable results.

10.1 Risk Assessment – Key Steps

Figure 1 highlights the key steps in an information security risk assessment process. At a high level, this includes the identification of the risk, assessment, and treatment, as well the communication and ongoing review and assessment of risks.

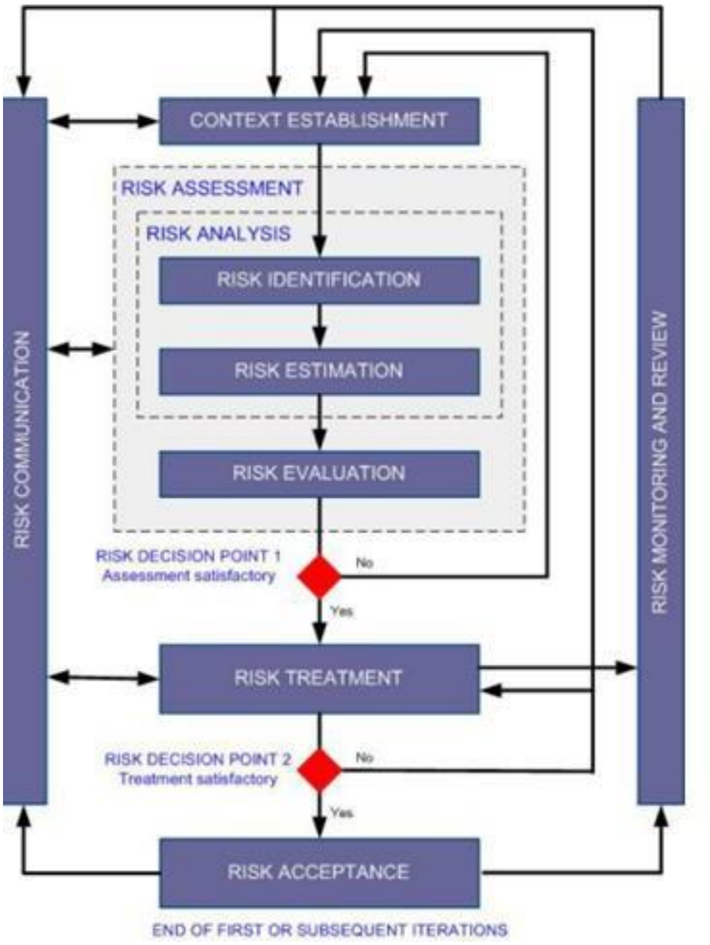

Figure 1: information risk assessment procedure

10.2 Likelihood Ratings

Likelihood Ratings	Rating #	Description
Almost Certain	5	The event will occur within the next 12 months.
Likely	4	The event will probably occur within the next 12 months.
Moderate	3	The event might occur over the next 12 months.
Unlikely	2	The event could occur sometime in the next 12-24 months.
Rare	1	The event may only occur in exceptional circumstances

10.3 Consequence Ratings

Impact Rating	Rating #	Confidentiality, Integrity, Availability
Very High	5	Loss of sensitive information International reputation impact. Monetary loss ($1m+)
Major	4	Loss of some sensitive information. National media impact. Monetary loss ($500k to $ 1m)
Moderate	3	Loss of some sensitive information. Moderate National media impact (a few occurrences) Monetary loss ($250k-$500k)
Minor	2	Loss of some sensitive information. Some National media impact (one occurrence) Monetary loss ($50k-$250k)
Insignificant	1	Loss of some sensitive information. Nil media coverage. Monetary loss (less than $50k)

10.4 Risk Matrix

IMPACT					
LIKELIHOOD	Insignificant 1	Minor 2	Moderate 3	Major 4	Very High 5
Almost Certain 5	Low -5	Medium -10	High -15	Critical -20	Critical -25
Likely 4	Low -4	Medium -8	High -12	High -16	Critical -20
Moderate 3	Informational -3	Low -6	Medium -9	High -12	High -15
Unlikely 2	Informational -2	Low -4	Low -6	Medium -8	Medium -10
Rare 1	Informational -1	Informational -2	Informational -3	Low -4	Low -5

10.5 Risk Ratings

Risk Ratings		
Score	**Risk**	**Action**
1 – 3	Informational	Report to the IT Security and Risk Officer to add the risk to the Risk Register and reassess annually.
4 – 7	Low	Report to the IT Security and Risk Officer to add the risk to the Risk Register and treat within 6 Monthly
8 – 11	Medium	Report to the IT Security and Risk Officer to add the risk to the Risk Register and treat within 3 Months
12 – 19	High	Report to the IT Security and Risk Officer to add the risk to the Risk Register and treat within 1 Month
20 - 25	Critical	The risk is outstanding and threatens the whole of the operations. It must be reported immediately to the senior management and treated immediately.

11. **Compliance**

All *Health Services Union* officers and personnel, including full-time, temporary and third-party employees, with access to IT resources must adhere to this policy. The *Health Services Union undertakes* monitoring of IT resources. Deviation from this policy may be permitted with advanced approval in writing by Human Resources Manager.

It is a requirement that all staff have read, understood and agree to abide by this policy and all other Security Policies as a condition of employment. Staff will be asked to sign a copy of each of these documents before access is granted. For existing staff who already have access to these services, you will be provided with a timeframe for reading these documents and asked to sign a copy and return to the IT Department. This signed document will serve as an acknowledgement that you have read the Policy and Guidelines and agree to abide by them.

Employees found to have violated this policy will be disciplined as per *Health Services Union's* Human Resources policies. Corrective actions could include, but are not limited to:

- revoking or restricting any right to use IT systems and equipment, such as email or Internet;
- corrective action, warning or cautioning; or
- Termination of employment.

If employees' behaviour constitutes a criminal offence, then appropriate legal action may be taken. Breaches to this policy can be reported to Human Resources Manager in writing.

Third parties found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

12. Documentation required with this Policy

Documentation	Description
Wireless Access Point Register	Documented inventory records of authorized wireless access points must be maintained, and a business justification is documented for all authorized wireless access points.
Software List	A List or a Register of Approved Products and correctly licensed Software permitted for use within the *Health Services Union* List of software running on server shall include operating system, programs, and services running on the server.
Hardware List, Network, Router, Server List	An up to date register of all IT equipment. This includes listing of all routers, along with the access controls provided by each router, be maintained.
Data Center and Storage	All computer hardware and associated peripheral equipment will be marked with a unique asset tag. Labelling should include information such as owner, contact information, and purpose.
Configuration Settings	The minimum requirements for configuration settings and rules for routers, switches, IDS/IPS and firewall devices is required to be documented, including permitted protocols, services, source and destination addresses etc. shall be reviewed and updated at least annually or when significant changes occur. Listing of all routers, along with the access controls provided by each router, must be maintained.
Data Classification	Data classification information shall be documented, reviewed, approved and disseminated to all staff. Policy shall include Labelling, Retention, Media Handling and Destruction process and procedures
Network Diagrams	Network diagram showing cardholder data flows over the network must document all connections to cardholder data, including any wireless networks and must be maintained, reviewed and kept current.
System Configuration Standards	Document System Configuration Standards for all system components that are consistent with industry accepted System Hardening Standards. A Configuration Standard policy should define how system components are configured to the particular function that is required. Document should show services and port enabled / disabled, list what accounts and password types should be created; or can be very detailed and list step by step how to setup a system component. However, the document should be in line with industry accepted hardening standards and should include instructions for testing that the required hardening has been achieved.
Business Justification for enabled services	Application or system services not being used for a defined business purpose must be disabled, including any part of the operating system that is unnecessary to the business purpose of the system. (E.g. daemons, "insecure" protocols). If ports, services, daemons, or protocols that are considered "insecure" are being used they need to be justified and security features need to be documented. Additionally, an evidence of security features and controls implemented to mitigate the associated risks must be provided.)
Patch Management	All associated procedures and procedural steps and roles and responsibilities for Patch Management.

Roles requiring Access to display of PANs	A list of roles that need access to display of full PAN must be maintained and documented, together with a legitimate business need for each role to have such access.

13. Glossary

Term	Definition
Cardholder Data (CHD)	At a minimum, cardholder data contains the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: Cardholder name Expiration date Service Code Full magnetic stripe data (track data) – This information is considered sensitive and must never be stored, even if encrypted CID/CAV2/CVC2/CVV2 (see definition below) – This information is considered sensitive and must never be stored, even if encrypted Pin/Pin Block – This information is considered sensitive and must never be stored, even if encrypted
Cardholder Data Environment	A specific computer system network that stores, processes or transmits cardholder data or sensitive authentication data, and those systems and segments that directly attach or support this environment without segregation controls.
Payment Card Industry (PCI) Data Security Standard (DSS)	Industry standard outlining twelve security requirements applicable to organisations that store, process or transmit payment card information.
Service Code	Three- or four-digit value on the magnetic stripe used for Payment Card Industry purposes.
Users	The term Users refers to all *Health Services Union* employees, volunteers, contractors and authorised individuals who use or have access to any of *Health Services Union information* systems, data (regardless of media or form) and physical premises.