A close-up of a blue and purple gradient

Description automatically generated

Information Security Policy

May 2024

Contents

[How to use this guideline and template 2](#_Toc161997937)

[Policy statement 3](#_Toc161997938)

[Policy review and updates 3](#_Toc161997939)

[Scope and applicability 4](#_Toc161997940)

[Enforcement and consequences 4](#_Toc161997941)

[Roles and responsibilities 5](#_Toc161997942)

[Information classification and handling 6](#_Toc161997943)

[Information security risk assessment and management 7](#_Toc161997944)

[Access control and passwords 8](#_Toc161997945)

[Incident response 9](#_Toc161997946)

[Security awareness and training 9](#_Toc161997947)

[Physical security 10](#_Toc161997948)

[Supplier management 10](#_Toc161997949)

[Monitoring and auditing 11](#_Toc161997950)

[Technology security 12](#_Toc161997951)

[Business continuity and data backups 12](#_Toc161997952)

[Compliance and legal requirements 13](#_Toc161997953)

|  |
| --- |
| An Information Security Policy (ISP) provides an overview of management’s approach to information security practices that reduce the risk to confidentiality, integrity and availability for an organisation’s systems and information. An effective ISP will lay out the areas of information security risk that have been considered for an organisation, and give an indication of how these risks are being addressed. |

# How to use this guideline and template

This document is a starting point for your Information Security Policy. It will assist you in the development of an information security policy that meets your organisation’s needs and follows the Health Information Security Framework (HISO-10029:2023) guidance for micro-small organisations provided by Te Whatu Ora.

This template has been provided at a detailed level to support a comprehensive document that includes all the 21 requirements that HISF (Health Information Security Framework) recommends for micro-small organisations. Some organisations may wish to have a high-level Information Security Policy and develop separate policy documents with more details for specific requirements. For example, the topics of Incident response and Business Continuity and Data Backups are recommended to be detailed in separate documents, as cyber security is only one aspect of these topics, and an organisation is likely to already have a detailed policy in place.

Guideline information is provided in purple and sample content in standard text. Guidance information should be removed after this template is completed, and blue typeface content should be overwritten.

There are references within this document to other supporting documentation that may or may not be available from Te Whatu Ora. These references may need to be removed if your organisation does not have these documents.

The relevant HISF statement has been noted to provide connection to additional HISF resources, should more detail be needed on the guidance for a specific topic.

# Policy statement

State the purpose of the policy, emphasising the importance of information security within the organisation. Express management’s commitment to protecting information assets.

The purpose of this policy is to define Organisation’s information security requirements with the following objectives:

1. Provide management direction and express management’s commitment for the support for information security.
2. Support the security requirements of Organisation to protect information assets from risks due to the loss of confidentiality, integrity, and availability.
3. Articulate to individuals and organisations the consequences of policy violations.

The board’s approval for the use of this policy is documented and the board participates in its annual review.

Related Requirement: HMS02

# Policy review and updates

Establish a schedule for reviewing and updating the policy, considering changes in your business needs, technologies, threats, regulations, and organisational structure.

On an annual basis, this and all security policies will be reviewed by policy owners and management, and may be updated considering:

* Changes in business needs for Organisation.
* Changes in technologies that are used by, nor longer used by, or may impact Organisation.
* Threats to the organisation, from both external and internal sources.
* Regulation changes that will impact Organisation.
* Modifications to Organisation’s structure which will impact security.

# Scope and applicability

Define the scope of the policy in terms of the locations, systems, resources, and users it applies to, including outlining specific goals and objectives.

The locations that are included in the scope of this policy are:

* Name of business, 123 Street Name, Town/City

The systems that are included in the scope of this policy are:

* Name of system(s)

This policy applies to all individuals (employees, contractors, vendors, volunteers, officers) who are authorised to access these systems and information.

Related Requirement: HMS03

Related Resources: Asset Management Worksheet for Micro/Small Organisations

# Enforcement and consequences

State the consequences of policy violations, including disciplinary actions, legal actions, or other appropriate measures. If there are any exceptions to the policies, document them with reason, approvals, and timeframes.

All managers and supervisors are responsible for enforcing the provisions of this document.

All individuals named within the scope of this document and who violate these policies and procedures may be subject to disciplinary procedures up to, and including, termination.

We follow our personnel process for managing policy violations, which includes documented report of the policy violation, the date it occurred, subsequent communication with the violator.

# Roles and responsibilities

Outline the responsibilities of all roles involved in information security, including directors, managers, clinical staff, administrative staff (including third party contractors), and any other relevant parties. Define who is accountable for policy enforcement, regular assessments, and incident response. Responsible individuals can delegate tasks to others; however, they ultimately remain accountable.

|  |  |
| --- | --- |
| Board | * Confirm information risk is managed to an agreed level. * Review and sign-off on Information Security Policy. |
| Owner / Directors | * Lead an information security risk assessment and ensure tasks are assigned to accountable parties. * Periodically review suppliers and staff to confirm compliance to security policies. * Provide guidance and leadership during response to incidents. |
| Practice / Business Manager | * Confirm all staff are trained in security awareness, policies, and procedures as part of their induction. * Confirm annual security awareness refresher training is held for all staff. * Monitor and address operational security policy compliance issues. |
| IT Supplier | * Provide technology services that meet security requirements, based on agreed to and contractual service levels. |
| Staff | * Follow all relevant security policies and procedures. * Report any suspect security concerns. |

Related Requirement: HMS01: Roles and Responsibilities

# Information classification and handling

Define how information will be categorised based on its sensitivity and value. Outline guidelines for managing this information by considering access controls, encryption, storage, transmission, and secure disposal.

Information will be classified based on sensitivity, value, and legal requirements. The level of security will reflect the classification of the information.\*

* Patient information: MEDICAL IN-CONFIDENCE.
* Staff personal information: STAFF IN-CONFIDENCE.
* Organisation Financial, Contractual information: COMMERCIAL IN-CONFIDENCE.
* Publicly available information – UNCLASSIFIED.

Security controls for each classification will consider, at a minimum:

* Access controls:
  + Appropriate processes for authorising access.
  + Technology to prevent unauthorised access (passwords, multi-factor authentication).
* Requirements for encryption when storing or transmitting.
* Locations where information can be stored (e.g. shared drives, removable drives).
* How information is securely disposed of (e.g. paper records or hard drives).
* Requirements for data backup and recovery.

\*These labels come from the New Zealand Protective Services Requirements guidance. https://protectivesecurity.govt.nz/

Related Requirement: HMS06

Related Resources: Asset Management Worksheet for Micro/Small Organisations

# Information security risk assessment and management

Detail the process for identifying, assessing, and managing information security risks. Explain how risk assessments will be conducted, including identifying threats, vulnerabilities, impact analysis, and risk treatment strategies.

An information security risk assessment is conducted on an annual basis. The high-level steps of our process include:

1. Information is categorised (by sensitivity or value, etc) and the location of the information is identified.
2. The threats to the confidentiality, integrity or availability of the information are identified and the risks are documented, noting the likelihood and impact should the risk become an actual incident.
3. The risks are prioritised and risk treatment plans are identified, with actions assigned to individuals to complete within a given timeframe.
4. Risk treatment actions are monitored and enforced.
5. On an annual basis, all risks are reviewed and updated for relevance and treatment.

Related Requirement: HMS05

Related Resources: Technology Risk Assessment template for Micro/Small Organisations

# Access control and passwords

Describe the principles and procedures for granting, modifying, and revoking access to information systems, networks, and information. Discuss authentication mechanisms, such as passwords, role-based access, such as nurse or staff account types. Discuss the principle of least privilege – only giving access to information that is required to complete one’s job.

Address how passwords are to be set (e.g., complexity, minimum password length, password expiry). Mandate changing of default passwords on all systems and applications.

All staff and contractors have employment verification screening before being given access to facilities or systems.

Requests for system or information access follow a formal process and are documented. Access is only provided as needed to fulfil the role of the individual at Organisation.

Access is removed when it is no longer required, or when contractual agreements expire.

Technical controls, such as passwords and multi-factor-authentication, including password complexity and refresh, follow best-practice standards. All default passwords are changed by system or account owners.

Neither accounts nor passwords may be shared, and staff are trained to follow this policy as part of the onboarding security training.

Periodic audits of users (including employees, contractors, vendors, volunteers, and officers) accessing all systems will be completed by an accountable system owner.

Related Requirement: HMS06 HMS07

# Incident response

Create a detailed incident response plan defining the steps to be taken in case of security breaches, data leaks, or other incidents (including roles, communication protocols, containment, investigation, and recovery procedures).

Management has created a documented cyber incident response plan, and the plan has a regular review, at a minimum, in line with the review of this policy.

We log all access to health information and store these logging records securely (encrypted, offline) for a period in case we need to analyse this information. Only those individuals with the authority to review these logging records are given access.

Related Requirement: HMS18 HMS20

Related Resources: [Te Whatu Ora Cyber incident advice for Primary Healthcare](https://www.tewhatuora.govt.nz/our-health-system/digital-health/cyber-hub/cyber-incident-advice-for-primary-health/)

# Security awareness and training

Emphasise the importance of ongoing security awareness and training for personnel. Detail the topics covered, frequency of training sessions, and methods of delivery. Training should cover a wide range of security topics, including data protection, email security, and safe internet browsing, highlighting risks of weak passwords, sharing access, and phishing attacks.

A designated person is responsible for security training.

We provide security awareness training to any staff or contractor who has access to our systems in the following manner:

1. We have a security video that all new staff or contractors must watch.
2. We provide a check list for how to securely work remotely, and have a documented acceptance that remote workers have read, understood, and follow the checklist.
3. On an annual basis, we hold a security meeting that all staff or contractors must attend, where we review security risks and have a 10-question quiz at the end.

We review:

* 1. Legal requirements for privacy and data sharing
  2. Phishing and other email security
  3. Restrictions and requirements for internet access
  4. Social media restrictions
  5. Best practice for password protection.

1. On an annual basis, all staff sign our Acceptable Use policy, which includes their responsibilities for following our security policies.

Related Requirement: HMS19

# Physical security

Address the physical security of your premise, including all entries and exits, removing access for personnel who have left the organisation, monitoring access to restricted areas, installing CCTV cameras (as required), and managing visitors.

All offices have keyed locks, and we track who has keys to the doors.

Our servers and patient record files are kept in locked cabinets and keys are only provided to those who need access for their job.

Staff are trained to not leave patient files visible, unlocked or outside their control. Staff should be encouraged to use privacy screens on computers in public view, and lock computer screens when away from their desks.

We have a remote work checklist that must be acknowledged in writing before we provide laptops, phones, or remote access to staff.

Related Requirement: HMS13

# Supplier management

Define the criteria and procedures for evaluating and managing the information security practices of suppliers who have access to your organisation’s systems and information.

Before purchasing any software, technology or giving information access to suppliers, a review process is conducted:

* The supplier must show how they meet HISF security standards or equivalent security standards.
* The supplier must meet our organisational needs for availability, functionality, or other requirements.
* There must be a formal contract, which shows the supplier’s responsibilities, including their responsibility if there is a breach of confidential information relating to their service.
* The contract and service level are reviewed on a regular, but no less than annual, basis.

Related Requirement: HMS04

Related Resources: Evaluating IT Supplier, Evaluating SaaS, Contractual Clauses

# Monitoring and auditing

Describe the monitoring mechanisms that will be used to track compliance with the policy and detect potential security breaches. Discuss regular security audits and their objectives.

Organisation is vigilant in terms of continuously monitoring the organisation, systems, and information for potential or actual cyber security incidents. This includes, at a minimum:

* Training all staff to be observant of unusual activity relating to systems and information, for example, suspected phishing emails, and training staff how to report any concerns.
* Audits of who has access to or has accessed systems and information on a regular – and at least monthly – basis, to reduce the risk of unauthorised access.
* Review of cyber security incidents, including violations of security policy, to determine whether corrective actions should be taken to reduce the risk of future incidents.
* Automated alerts, such as system logins from unexpected locations, where possible.

Related Requirement: HMS19

# Technology security

Specify the technical and organisational security measures that need to be implemented, including firewall configurations, intrusion detection, encryption protocols, and anti-malware measures. Alternatively, this section may call out the responsibilities of your IT supplier.

Organisation effectively manages the technology that is our responsibility, including:

* Ensuring all phones, laptops, workstations, servers, or other organisation-owned devices have patched, secure operating software, anti-malware software and only allow authorised and legal software to be installed.
* All technology networks are configured to be secure, including protection from unauthorised access by devices or individuals, encryption of information, and separation of health-related information from other information.

Public facing websites are built securely, using firewalls, encryption, public cloud services and other technical security protocols.

* Related Requirement: HMS08, HMS10; HMS14, HMS17, HMS09, HMS12, HMS15, HMS16
* Related Resources: Evaluating IT Supplier, Evaluating SaaS supplier

# Business continuity and data backups

Specify the technical and organisational security measures that need to be implemented, to ensure data is protected and the organisation can continue to function, should a serious cyber security event occur.

Critical information systems have a backup plan in place which states who is responsible for data backups; how often the data backups are created; where the data backups are stored; and who has access to the data backups. All data backups are encrypted.

Data backups are periodically restored to ensure they continue to serve the purposes of Organisation.

Organisation has determined its requirements for business continuity for critical functions during a disruption. And a separate Business Continuity Plan exists.

Related Requirement: HMS11, HMS21

# Compliance and legal requirements

List the relevant laws, regulations, and standards that your organisation must follow, including how the organisation will ensure compliance. Some organisations may choose to consolidate policies (e.g. Information Security and Privacy Policy containing all relevant requirements.)

Management has reviewed applicable laws, regulations and standards and has determined it will address compliance with:

* Example: Industry Regulations (Pharmacy Guild, RNZGP, etc)
* Example: Health Care Regulations (Privacy Act, Health Act))
* Example: Security Standards (HISF, NZISM, ISO 27001)

Related Requirement: N/A