****

**Information Security Management Plan:**

**[Insert Name]**

**Effective Date: [Insert date]**

Document control:

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Changes** | **Author** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Review and approval:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Name** | **Signature** | **Date** |
| Prepared by: |  |  |  |
| Reviewed by: |  |  |  |
| Reviewed by: |  |  |  |
| Reviewed by: |  |  |  |
| Approved for publication by: |  |  |  |

Table of contents

[1. Introduction 4](#_Toc374359285)

[2. Purpose and scope 4](#_Toc374359286)

[3. Roles and responsibilities 4](#_Toc374359287)

[4. Vulnerability analysis 5](#_Toc374359288)

[5. Change control 5](#_Toc374359289)

[6. Business continuity and disaster recovery 6](#_Toc374359290)

[7. Physical security of facilities 6](#_Toc374359291)

[8. Privileged access 6](#_Toc374359292)

[9. Removable media usage 6](#_Toc374359293)

[10. Media destruction 6](#_Toc374359294)

[11. Hardening of operating environments 7](#_Toc374359295)

[11.1 Hardening of databases 7](#_Toc374359296)

[11.2 Hardening of servers 7](#_Toc374359297)

[11.3 Hardening of workstations 7](#_Toc374359298)

[12. Product patching and updating 8](#_Toc374359299)

[13. Web applications and web application development [if applicable] 8](#_Toc374359300)

[14. Software application development [if applicable] 8](#_Toc374359301)

[15. Identification and authentication 8](#_Toc374359302)

[16. Event logging and auditing 8](#_Toc374359303)

[17. Network security 9](#_Toc374359304)

[18. Email infrastructure [if applicable] 9](#_Toc374359305)

[19. Intrusion detection and prevention [if applicable] 10](#_Toc374359306)

[20. Secure electronic transmission of data 10](#_Toc374359307)

# Introduction

This plan governs the integrity, privacy, security, and confidentiality of [insert name]’s information, especially highly sensitive information, and the responsibilities of departments and individuals for such information. IT security measures are intended to protect information assets and preserve the privacy of [insert name]’s employees, students, sponsors, suppliers, and other associated entities. Inappropriate use exposes [insert name] to risks including virus attacks, compromise of network systems and services, and legal issues.

# Purpose and scope

The purpose of this plan is to describe how the confidentiality, integrity, and availability of information will be ensured through the implementation of IT security measures.

The University of Auckland’s information security policies and procedures represent the foundation for [insert name]’s information security plan. Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout the University. The information security policies adopted by the University can be found here <https://policies.auckland.ac.nz/staff-it.aspx>

Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in the operations of the business. When consistently applied throughout the University, these policies and procedures assure that information technology resources are protected from a range of threats in order to ensure business continuity and maximize the return on investments of business interests.

This plan reflects [insert name]’s commitment to stewardship of sensitive personal information and critical business information, in acknowledgement of the many threats to information security and the importance of protecting the privacy of University constituents, safeguarding vital business information, and fulfilling legal obligations. This plan will be reviewed and updated at least once a year or when the environment changes.

This plan applies to the entire [insert name] community, including the Dean, Directors, and Department Heads, students, staff, alumni, temporary employees, contractors, volunteers and guests who have access to [insert name] information technology resources. Such assets include data, images, text, or software, stored on hardware, paper or other storage media.

# Roles and responsibilities

Responsibility for information security is divided between central IT Services (ITS) and [insert name]’s IS department. ITS are responsible for the following:

* Monitoring and maintenance of firewalls
* Authentication and identity
* Responding to cyber and information security incidents
* Security of central email servers and web servers
* Security of the University network
* Security of servers hosted by ITS within the central University data centres
* Security of databases and applications for central services
* Setting of policies, standards and guidelines for security of networks, operating systems, databases and applications
* Detection of intrusions into the central University network
* Management of information security risk for University-wide systems
* Physical security of data centres

The IS department within [insert name] is responsible for:

* The security of servers maintained within [insert name], i.e. hardening of servers, applying patches, etc.
* Maintaining security of all networks set up within [insert name] (other than the central University network) in accordance with the policies, standards and guidelines set by ITS
* Advising ITS of any cyber and/ or information security incidents and assisting with resolving such incidents as required. Incident reporting is done in accordance with the University’s IT Incident Reporting Standard, which can be found here: [insert link]
* Security of all email and web servers set up within [insert name], other than the central University email and web services
* Security of applications and databases provided by [insert name]
* Management of information security risk within [insert name] and advising ITS of any high risks that could affect the University as well as [insert name]

# Vulnerability analysis

[Describe the plan for your faculty/ service/ research unit to conduct regular analyses of vulnerabilities. These should be conducted on at least an annual basis (and preferably more frequently), and can be performed by any of the following:

* Your unit’s own security team (not recommended, as this will lack objectivity)
* Central ITS Security
* External service providers, such as internal audit (would be ideal, but there will be a cost involved)]

# Change control

Change control is the process that management uses to identify, document and authori**s**e changes to an IT environment. It minimi**s**es the likelihood of disruptions, unauthorised alterations and errors.

[Describe the change control plan for your faculty/ service/ research unit, referring to:

* Change request initiation and control
* Assessment of impact
* Control and documentation of changes
* Roles and responsibilities for documenting, testing, authorising and implementing changes
* Version control
* Roll back plans
* Control over emergency changes]

# Business continuity and disaster recovery

[Insert name] provides a safe, secure IT environment to serve its customers’ requirements, ensure stability and continuity of the business, and promote confidence in its ability to not only continuously provide goods and/or services, but also to recover quickly from disaster and minimise disruption.

[Insert name]’s business continuity and disaster recovery plans can be found here: [insert link]

# Physical security of facilities

Physical security controls and secure areas are used to minimise unauthorised access, damage to, and interference with information and information systems. Physical access to servers and network devices within [insert name] is restricted to authorised individuals.

[Describe plan to restrict physical access to servers and network devices. In addition, also make reference to who will be authorised to access data centres on your business unit’s behalf. ]

For other information technology resources (such as laptops, tablet computers, etc.), the assigned user of information technology resources is considered the custodian for the resource. If the item has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, the custodian must promptly inform the [insert name] IS manager.

# Privileged access

Privileged access is considered to be access which can give a system user:

* the ability to change key system configurations
* the ability to change control parameters
* access to audit and security monitoring information
* the ability to circumvent security measures
* access to data, files and accounts used by other system users, including backups and media, or
* special access for troubleshooting the system.

[Describe plan for restricting privileged access]

# Removable media usage

Removable media are data storage devices capable of being removed from a computer system without powering off the system. Examples include: laptops, tablets, USB memory sticks/ flash drives, external hard drives, CD’s, personal digital assistants, mobile phones, or memory cards.

[Describe plan for usage of removable media. Reference must be made to virus protection and encryption/ password protection of sensitive data, specifically personal information. Reference should also be made to protection of information that is transported off-site. The plan also must contain detail on the persons to contact and the procedures to be followed in the event of loss or theft of removable devices. ]

# Media destruction

Proper data disposal is essential to controlling sensitive data including student records, personnel records, financial data, and protected health and credit card information. If the information on those systems is not properly removed before the equipment is disposed of, or transferred within the University, that information could be accessed and viewed by unauthorised individuals.

[Describe plan for ensuring proper data disposal.]

# Hardening of operating environments

If insecurely configured, operating environments provide opportunities for unauthorised access that could lead to fraud or disclosure of sensitive information.

## Hardening of databases

[Describe plan for hardening of databases. Reference should be made to:

* Removal of removal of unneeded software and operating system components
* Disabling of unused or undesired functionality in software
* Implementation of access controls on relevant objects to limit system users and programs to the minimum access required
* Configuration of either remote logging or the transfer of local event logs to a central server
* Removing unused accounts
* Renaming or deleting default accounts
* Replacing default passwords
* Preventing users from installing or disabling software without approval]

## Hardening of servers

[Describe plan for hardening of servers. Reference should be made to:

* Removal of removal of unneeded software and operating system components
* Disabling of unused or undesired functionality in software and operating systems
* Implementation of access controls on relevant objects to limit system users and programs to the minimum access required
* Installation of antivirus software
* Installation of software-based firewalls limiting inbound and outbound network connections
* Configuration of either remote logging or the transfer of local event logs to a central server
* Removing unused accounts
* Renaming or deleting default accounts
* Replacing default passwords
* Preventing users from installing or disabling software without approval]

## Hardening of workstations

[Describe plan for hardening of workstations. Reference should be made to:

* Removal of removal of unneeded software and operating system components
* Disabling of unused or undesired functionality in software and operating systems
* Implementation of access controls on relevant objects to limit system users and programs to the minimum access required
* Installation of antivirus software
* Configuration of either remote logging or the transfer of local event logs to a central server
* Removing unused accounts
* Renaming or deleting default accounts
* Replacing default passwords
* Preventing users from installing or disabling software without approval]

# Product patching and updating

[Describe plan for testing and applying security patches for both operating systems and applications. The plan should include references to monthly maintenance windows when patches are applied as part of other maintenance. For those systems that cannot be offline at any time, a high availability strategy must be included.]

# Web applications and web application development [if applicable]

Web applications provide potential entry points into the University’s systems if appropriate security measures are not put in place.

Web applications must be tested by ITS security for the presence of vulnerabilities and coding weaknesses prior to deployment in the University IT environment.

[Describe plan for securing web servers and web applications where these are hosted within your unit.]

# Software application development [if applicable]

Insecurely developed software applications provide opportunities for unauthorised users to make unauthorised changes and/ or gain unauthorised access to sensitive information.

[Describe plan for securing any applications developed within your unit. Reference must be made to reviewing and testing for vulnerabilities prior to deployment in a production environment and restriction of user access rights.]

# Identification and authentication

Identity and access management ensures accurate identification of authorised University community members and provides secure authenticated access to and use of network-based services. Identity and access management is based on a set of principles and control objectives to:

* Ensure unique identification of members of the University community and assignment of access privileges
* Allow access to information resources only by authorised individuals
* Ensure periodic review of membership in the community and review of their authorised access rights
* Maintain effective access mechanisms through evolving technologies

Identity information is recorded in the Enterprise Person Registry (EPR) database, while there are various authentication and authorisation services, depending on what is being accessed. These include Kerberos, LDAP, Active Directory and Shibboleth.

# Event logging and auditing

Event logging is essential for tracking and investigating security incidents.

[Describe plan for logging and auditing of events at operating system, database and application levels. Reference must be made to:

* Logging of:
	+ all privileged operations
	+ failed attempts to elevate privileges
	+ security related system alerts and failures
	+ system user and group additions, deletions and modification to permissions
	+ unauthorised access attempts to systems and files identified as critical to your unit
* Recording of:
	+ date and time of the event
	+ relevant system user(s) or process
	+ event description
	+ success or failure of the event
	+ event source (e.g. application name)
	+ IT equipment location/identification
* Protection of event logs from:
	+ modification and unauthorised access
	+ whole or partial loss within the defined retention period]

# Network security

Network attacks launched from the Internet or from University networks can cause significant damage and harm to information resources including the unauthorised disclosure of confidential information. In order to provide defensive measures against these attacks, firewall and network filtering technology must be used in a structured and consistent manner.

[Describe plan for ensuring security of networks maintained within your unit.]

# Email infrastructure [if applicable]

Email provides opportunities for the execution of malicious code, dissemination of content contrary to the University’s email policy or of sensitive information to unauthorised users, or attempts to obtain user credentials.

[If your unit provides email services in addition to those provided by central ITS, describe the plan for securing of emails. Reference should be made to blocking of:

* inbound and outbound email, including any attachments, that contain:
	+ malicious code
	+ content in conflict with the University’s email policy
	+ content that cannot be identified, or
	+ encrypted content, when that content cannot be inspected for malicious code or authenticated as originating from a trusted source
* emails addressed to internal email aliases with source addresses located from outside the domain
* all emails arriving via an external connection where the source address uses an internal University domain name.]

# Intrusion detection and prevention [if applicable]

Early detection and monitoring of intrusions can prevent possible attacks or minimise their impact on computer systems.

[If your unit provides intrusion prevention/ detection services in addition to those provided by central ITS, describe the plan for intrusion prevention/ detection. Reference must be made to:

* appropriate intrusion detection mechanisms, including network-based IDSs and host-based IDSs as necessary
* the audit analysis of event logs, including IDS logs
* a periodic audit of intrusion detection procedures
* cyber security awareness and training programs
* providing the capability to detect cyber security incidents and attempted network intrusions on gateways and provide real-time alerts.]

# Secure electronic transmission of data

It is sometimes necessary to transmit sensitive and/ or confidential electronic data to persons or organisations who do not have access to the University’s systems. Using unprotected email to transmit such data presents a number of risks, not the least of which is interception by unauthorised persons. In order to protect this data, it must be transmitted using secure means.

[Describe plan for secure electronic transmission of data.]