TOI OHOMAI INFORMATION SECURITY STANDARDS

Abstract

Document outlining the security standards for the selection, development, integration, management and maintenance of the information systems Toi Ohomai Institute of Technology

Document Owner: Rabindra Das

Contents

INTRODUCTION

Technology and Information are two of Toi Ohomai's key business assets both in terms of financial investment and business delivery, hence they also represent areas of considerable risk to the Institute.

For Toi Ohomai to operate effectively and efficiently, the information systems must remain reliable, available, and secure.

Toi Ohomai's reputation for quality and service must be maintained and enhanced to maintain competitive advantage in an increasingly global market for education services.

The risk of cybersecurity incidents is persistent and, by most measures, increasing year-on-year. Cybersecurity events can be accidental, targeted, or indiscriminate and opportunistic. The business impact of a cybersecurity event could include reputational damage, loss of customer trust, negative legal or compliance consequences and financial loss.

New Zealand privacy laws require us to store and process personal information in a diligent and responsible manner. Privacy expectations have been heightened with recent high-profile global breaches. Within New Zealand (and globally) laws are changing to meet peoples' expectation of privacy and to provide transparency when those standards are not met. Failure to meet these privacy laws and expectations is a threat to Toi Ohomai's reputation and, in the future, may have legal implications.

RISK ENVIRONMENT

Not all systems, facilities, and information at Toi Ohomai have the same level of risk. Some systems, networks and information are more critical or sensitive than others.

Understanding the Toi Ohomai risk environment is essential to focusing limited resources and making pragmatic, risk-based decisions.

Inherent risk for main environments

Inherent risk (shown below) is the risk of confidentiality, integrity or availability being negatively affected if there were no controls in place. It represents the raw risk to the Institute given its industry and technology footprint.

Institute environment		
Accidental[1]	**Opportunistic**[2]	**Targeted**[3]
		
MEDIUM	HIGH	MEDIUM

Student environment		
Accidental[1]	**Opportunistic**[2]	**Targeted**[3]
		
LOW	HIGH	MEDIUM

IT School environment		
Accidental[1]	**Opportunistic**[2]	**Targeted**[3]
		
HIGH	HIGH	LOW

- **Accidental:** Through a lack of training, diligence or care an employee or third party compromises the Confidentiality, Integrity or Availability of Toi Ohomai's technology or information. This could include, for example: inadvertently sending private records to the wrong external recipient or making an incorrect configuration change which breaks a critical service. Accidents are the most common form of insider threat.
- **Opportunistic:** Opportunistic attacks are the most common technology risk faced by a modern business. This is a crime of opportunity, not specifically targeting Toi Ohomai. It is in these cases that a solid cyber-defence can do the most to avoid incidents. The most common opportunistic attacks are from vulnerable Internet facing services (including API's, websites, etc.) and phishing (including ransomware, crypto mining & credential theft).
- **Targeted:** This sort of attack is categorised by intent and dedicated resources. There is almost no way to prevent a focused targeted attack by a competent adversary. Often a company's best hope is to slow an attack long enough to detect it. Often criminals behind this sort of attack work tirelessly with many resources to achieve their objective.

The goal is to achieve an appropriate balance between risk and the cost to address it.

BUSINESS PRIORITIES

- Protect the ability for Toi Ohomai to conduct normal business and teaching delivery.
- Protect Toi Ohomai students and staff information/privacy.
- Protect Toi Ohomai institutional assets and intellectual property, including our data.
- Protect Toi Ohomai's reputation.
- Demonstrate to stakeholders that Toi Ohomai has appropriate focus on cybersecurity.

SCOPE

The Toi Ohomai Information Systems Policy sets the formal mandate, responsibilities and high-level principles for the use of technology in the Institute and the associated security expectations.

This document (Toi Ohomai Information Security Standards) provides practical and more detailed guidance for the administrative, procedural and technical controls to deliver a secure computing environment for Toi Ohomai.

CLASSIFICATION LABELS

Some of the standards in this document only apply to certain information, systems, or facilities. When a policy to less that all classification levels, the specific standard will be prefixed with one or more of  ,  ,  or - relating to the classifications below.

 **Public**

Can be shared openly with any other parties (including competitors and the public).

Examples: Brochures, public reports, public website.

 **Institutional** [Default]

Institutional classification covers all information which is for internal or trusted third-party use only. All information, systems and facilities are classified “Institutional” unless otherwise classified.

Examples: Policies, internal correspondence, forms and templates.

 **Sensitive**

This usually relates to financial, employment or business strategy information which if misused could have significant reputation, legal, regulatory, or competitive implications. Access is usually role based.

Examples: Staff personnel files, student records, medical records, financial forecasts, capacity reports, government regulatory reporting.

1 INFORMATION SECURITY POLICY

The tone for information security is set by the executive and senior management layers in an organisation. *Management should demonstrate support for, and commitment to, information security, providing clear direction and support.*

1.1 Information Security Policy

- Toi Ohomai must establish the *Toi Ohomai Computer Systems Policy* to address all the information security requirements for the Institute.
- The *Toi Ohomai Computer Systems Policy* must:
  - clearly define the responsibility for all aspects of information security at the Institute.
  - be published and be communicated to all students, employees and relevant external parties.
  - be supported with standards, guidelines and procedures that provide adequate detail to implement the security policy.

1.2 Review of Security Policy

- All security policies, standards and guidelines should be reviewed every two years or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

2 ORGANISATION OF INFORMATION SECURITY

Securing an organisation's information assets requires a management framework. This structure will initiate and control implementation and operation of information security within the organisation.

Clearly defined and allocated responsibilities for information security are the key to a unified and successful information security effort.

2.1 Governance of Information Security

Toi Ohomai governs information security using the following formal groups and processes

2.1.1 Toi Ohomai Information Technology Governance Group (ITGG)

- The IT Governance Group *(refer ITGG Term of Reference)* is a body of senior Institute leaders. It makes decisions and sets direction pertaining to all technology matters. It is the governing body for consideration of risk exposures and monitoring of risk management.

2.1.2 Toi Ohomai Technical Security Forum (TSF)

- The Technical Security Forum *(refer TSF Terms of Reference)* is a group of technical people and subject matter experts who manage the technical security considerations for IT operations, architecture and new initiatives. The TSF meets 6 weekly and reports to the ISGG.

2.1.3 Management of Risk

- The Executive Director, Corporate Services is responsible for the establishment and maintenance of the institute's corporate risk register.
- The ITGG is responsible for the establishment and maintenance of the ICT risk register.
- The IT risk register must be reviewed every 6 weeks by the ITGG.
- The ICT risk register must, for each risk, include the following details:
  - Name
  - Date
  - Description
  - Threat
  - Impact
  - Likelihood
  - Vulnerability
  - Risk rating
  - Risk owner
  - Review date
- The risk owner is responsible for managing the risk and initiating action to mitigate the risk to bring it to an acceptable level.

2.2 Information Security Activities

- The *Toi Ohomai Information Technology Policy* details the formal responsibilities for information security.
- Staff members responsible for day-to-day activities that pertain to information security must have appropriate detail in their *Toi Ohomai Position Descriptions*, amplified and supplemented with written and verbal instructions and on the job training.
- Overall management and authority for all security related activities remains the responsibility of the Head of IT.

3 ASSET MANAGEMENT

To ensure that information is properly protected, it is important that the physical assets which process, store and transport information are properly accounted for.

Additionally, the information itself is an asset for the organisation. Information should be classified and labelled to ensure that it receives protection appropriate to its value.

3.1 Acceptable use of assets

- All users of Toi Ohomai's ICT resources must adhere to the Toi Ohomai Acceptable Use Guidelines

3.2 Information classification

Not all systems, facilities, and information have the same security requirements. Some systems, networks and information are more critical or sensitive than others.

3.2.1 Security Classification Levels

- Information will be classified and labelled with one of the following classifications:
  -  Public
    Can be shared openly with any other parties (including competitors and the public). For example: Brochures, public reports, public website.
  -  Institutional [Default]

    Institutional classification covers all information which is for internal or trusted third-party use only. All information, systems and facilities are classified "Institutional" unless otherwise classified. For example: Policies, internal correspondence, forms and templates.
  -  Sensitive

    This usually relates to financial, employment or business strategy information which if misused could have significant reputation, legal, regulatory, or competitive implications. Access is usually role based. For example: Staff personnel files, student records, medical records, financial forecasts, capacity reports, government regulatory reporting.

3.2.2 Classification labelling

- All information should be labelled with its classification, preferably in the file meta-data.
- Unlabelled information is assumed to be classified  Institutional by default.

3.2.3 Initial Classification

- As information sources, systems, or facilities (collectively described as "assets") are established, they are to be classified by the Executive Leadership Team member who owns the asset (the "data owner").
- If the owner of an asset is unable to decide, then the IT Governance Group will assign a classification.
- All classifications are to be notified to the IT Governance Group.

3.2.4 Classification review

- Classifications are to be reviewed every 36 months by the asset owner.
- The results of the re-classification are to be notified to the Information Technology Governance Group

3.3 Inventory and Control of Hardware Assets

- Discovery tools will be used to identify devices connected to the Institute's network and update the hardware inventory
- DHCP logging will be used on all DHCP services to update the hardware inventory.
- A detailed, accurate and up-to-date inventory of all technology assets that can store and process information. This includes all assets whether connected to the network or not.
- Hardware asset inventory records will include the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.
- Port level access control following 802.1x standards will ensure only authorised devices from the hardware inventory can connect to the network.

3.4 Inventory and Control of Software Assets

- An up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system will be maintained.
- Only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
- Software inventory tools will be used throughout the organization to automate the documentation of all software on business systems.
- The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.
- Unauthorized software should be either removed or the inventory updated in a timely manner.

3.5 Information management and data protection

Toi Ohomai will work to prevent data exfiltration and ensure the privacy and integrity of sensitive information. The institute will track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets.

- An inventory of all sensitive information stored, processed, or transmitted by the organisation's technology systems, including those located on-site or at a remote service provider will be maintained.
- Any very sensitive data or systems not regularly accessed by the organisation should be removed from the network. These systems shall only be used as stand-alone

systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualised and powered off until needed.

- Business data stored on mobile devices must be protected using approved cryptographic mechanisms.
- If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.
- Users will store all documents/files/records in the appropriate corporate repository. Examples include teaching/learning platforms, corporate document repository, HR management information system.
- Users must minimise version sprawl and duplication.
- [] Data owners must be identified for all Sensitive information. The data owner should be a member of the Leadership Team.
- [] Where practical, access to institutional information should be Protected based on a user's role.
- [] Access to Sensitive information will be protected based on the principle of least privilege (need to know) and assigned to specific role(s) and/or individuals.
- [] Sensitive information must contain "Sensitive" in the filename or a parent folder name.
- [] Sensitive information must never be sent/stored outside the approved Toi Ohomai corporate repositories without the written approval of the data owner.
- [] Third parties exposed to Sensitive Toi Ohomai information are required to sign a confidentiality or non-disclosure Agreement to the satisfaction of the data owner.
- The network will be segregated into security zones and VLANs with similar security requirements.
- Firewall filtering will be configured between VLANs to ensure that only authorised systems are able to communicate with other systems, as necessary.
- Information will be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorised individuals should have access to the information based on their need to access the information as a part of their responsibilities.

4 ACCESS CONTROL

Access to information and information processing systems must be properly controlled to protect the information. This includes registering users to use systems, the provisioning of access permissions and system privileges, the review and removal of access permissions and, ensuring that authentication mechanisms are appropriate to protect the information and systems.

4.1 Guiding principles for access control

- All people and systems who require access to information (and the systems which transport, store or process it) must be properly identified, authenticated and authorised.
- **Least privilege:** Access privileges for any user should be limited to resources and information essential for completion of their duties, and no more.
- **Separation of Duties:** Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.
- **Role Based:** Access is provided (and revoked) based on the user's role at Toi Ohomai. All access other than what is required for the role is unauthorised unless formally approved.
- **Single Authentication and Authorisation Engine:** Toi Ohomai will strive to reduce authentication and authorisation engines and services. Federation and single sign-on technologies will be leveraged wherever possible to reduce the number of user-identities associated with each human.

4.2 Account lifecycle

- All access requests must be requested using the appropriate Access Request form.
- Each account should only be associated with a single person or system. Shared accounts must be avoided.
- New accounts must be created using a strong unique temporary password. The initial password must force a password change at first logon.
- New IT/Privileged users (including contractors) must read and acknowledge the *Toi Ohomai Information Technology Policy* and *Information Technology Security Standards* before being granted access to Toi Ohomai's systems.
- New standard users must be made aware of the policy's existence and have read and acknowledged the *Acceptable Use Guidelines*.
- Where a user forgets their password and asks for it to be reset, the technician must satisfy themselves that the user requesting the password reset is genuinely the owner of the account. The temporary password must be set to force a password change at first login.
- Self Service Password Reset technology is preferred for user password resets
- Accounts must be disabled and authorisation to access systems must be revoked immediately when the account holder finishes their engagement with Toi Ohomai.

- Accounts provided to contractors or fixed term staff must have an expiry date aligned to the end of their engagement with Toi Ohomai (by month's end).
- Accounts issued to a user must never be used for automation.
- Disabled staff accounts must be retained for a minimum of 200 days before they may be deleted. This allows time to ensure that log entries and permissions can be mapped back to the account and to allow time for an extension to the account holder's engagement with Toi Ohomai.
- Disabled student accounts may be deleted after 90 days.

4.3 Roles and Access Permissions

- Role based access control must be used to secure resources.
- Accounts must be configured with the minimum permissions required to fulfil the accounts purpose (principle of least privilege).
- [🪪] Access to Sensitive information must be formally approved by the information owner. A request may be initiated by an email to the IT team, who will forward the request to the appropriate manager for approval before granting access. For clarity, this includes access to sensitive information held in or cloned to test and development systems.
- Access permissions (including role/group/scope assignments) must be reviewed and adjusted when an account holder changes role.

4.4 Identity Providers

- All Toi Ohomai's owned or operated systems, which require Identity & Access Management, must be linked to one of Toi Ohomai's approved identity provider platforms Linking must be achieved using an industry standard, encrypted, protocol such as Kerberos, LDAPS, or SAML 2.0.
- All Toi Ohomai's Internet exposed API's must use OAuth 2.0 and/or OpenID Connect (OIDC) standards linked to the Toi Ohomai's approved Authentication Platform.

4.5 Account Credentials

- Note: These clauses include Toi Ohomai controlled IAM platforms, as well as Toi Ohomai's accounts on 3rd party services.
- All Toi Ohomai user accounts are to be protected by a set of credentials, comprising a Username (Identifier), Password (Secret) and a second authentication factor.
- Toi Ohomai credentials must not be used on different systems (except under federated logins).

Criteria	Staff	Privileged	Service	Student
Complex password required	No	No	Yes	No
Minimum length	14	14	32	10
Minimum age (days)	1			
Maximum age (days)	365	365	No limit	365

Number of passwords remembered	12			
Failed attempt before lockout	5			
Lockout duration (minutes)	60			
Password self-service reset	Yes	Yes	No	Yes
Known bad password protection (e.g. Azure AD Password Protection)	Enabled			
Azure Smart lockout	Enabled			
Multi factor authentication	Required	Required	Disabled	Optional

- Where technically feasible, the following minimum requirements apply to one-time passwords and device PIN codes:

PIN and OTP Requirements	
Minimum Length	6 characters
Password complexity	Minimum of numeric only
Account lockout	10 Unsuccessful login attempts within 24 hours
Lock-out duration	Permanently until unlocked by IT team

- Acceptable second authentication factors are:
  - Mobile device push approval message (e.g. Duo, Microsoft Authenticator)
  - Hardware based one-time-password (e.g. YUBI key)
  - Application time based one-time-password (e.g. Google/Microsoft/Duo Authenticator)
  - Approved x509 certificate issued to a user or device by the Toi Ohomai Certificate Authority
  - SMS/TXT
  - Phone call
- Users will be supported to use a robust encrypted personal Password Manager for their personal credentials.
- Where applicable, users will be provided a Toi Ohomai approved Password Manager for their business units' shared credential storage.
- Passwords (including hashes), secrets, tokens, etc. are never to be stored in plain text (unencrypted). This includes, for example, in configuration files, on paper, or in spreadsheets.

- No device should be placed on the network until its default administration credential(s) have been changed.

4.6 External Credentials

- Where external parties are using Toi Ohomai's systems (e.g. a business-to-business system), the external party must use credentials that are compliant with this standard.
- Where an external party is using federated logins, then their password policy must be reviewed by Toi Ohomai to ensure it is compliant with this standard.

4.7 Privileged Accounts

Privileged accounts are accounts with more rights on a system than a standard user has. For example, root, administrator, SA and service accounts for applications and databases. This includes privileged Toi Ohomai accounts on 3rd party services.

- Creation and use of a Privileged Account requires formal approval by one of the following:
  - Head of IT
  - Executive or Manager responsible for the system's security.
  - Technical Services Manager
- All privileged accounts must adhere to the same requirements as a standard account.
- In situations where group accounts or shared passwords are required, the password must be changed immediately upon any personnel change within the group. MFA tokens for generic accounts must be held by the Technical Service Manager.
- Users who hold a standard and a privileged account must always operate in their standard account until a specific task requires the use of the elevated account. The elevation of privileges must only last for the duration of the task and then the user must revert to their standard account.
- Service accounts must not be used to log on to systems by system administrators, except to troubleshoot an error in the context of the service account.
- Service accounts must only have the minimum privileges required to perform their function.
- Service account passwords must be created using a password generator tool to ensure that password is truly random.
- Assigning domain administrator rights to a service account requires the approval of the Head of IT or the Technical Service Manager.

4.8 Accounting and Record Keeping

- All IAM requests must be recorded in the IT team's service management tool. This must include a record of who approved the request.
- A biannual review of all users shall be undertaken to validate an effective account lifecycle process.
- A biannual review of Domain and Enterprise Administrator group membership will be conducted to ensure effective rights management.

4.9 Session timeouts

- User sessions left inactive for a period of 15 minutes must be automatically logged out or locked unless the device and account have been specifically designed and secured for kiosk functionality.
- Administrator sessions left inactive for a period of 15 minutes must be automatically logged out or locked.

4.10 API security

- Toi Ohomai built APIs (except for those covered by in the next clause) must use OAuth 2.0 and OpenID Connect (OIDC).
- Internal-to-internal APIs which meet the criteria below may use OAuth 2.0, OIDC or static API tokens.
  - API calls are within a private network (not over the Internet).
  - API calls are within the same trust zone.
  - The APIs function cannot result in loss or degradation of service.
  - The API cannot affect the integrity of business records.
  - The API does not contain or return sensitive data (including personally identifiable information).
- Static API tokens should be generated, validated and/or revoked using a centralised key management platform which resides in the same or higher trust zone as the API.
- OAuth tokens are to be passed as JSON Web Tokens (JWT) using JWS compact serialisation, no compression and no JWS encryption (JWE).
- JWTs must use a secure algorithm. JWT's without an algorithm must be rejected.
- JWTs must be validated at the time of use.
- JWT expiry times must be set based on the level of risk associated with the scope(s) of the token. Tokens must not exceed 1 hour of validity.

- Scopes must be documented and follow [service]:[CRUD or method]:[authorisation] naming standard.
- OAuth Authorisation endpoints and audience must be unique between environments (Development, Test, Production).
- Credentials and tokens must be encrypted in transit (e.g. using TLS v1.2+).

4.11 Remote access, telecommunications and mobile computing

The Institute supports the development of a mobile workplace for its staff.

4.11.1 Devices that belong to Toi Ohomai

- Remote access to Toi Ohomai's systems (across the Internet) is enabled for all staff using a Toi Ohomai issued laptop unless otherwise requested by their manager.
- Only approved remote access technologies configured by the IT team may be used for connecting to Toi Ohomai's networks or systems.
- Approval to be issued with a mobile device must be given by a member of the Leadership Team
- Mobile devices that are to be connected to or synchronised with the Toi Ohomai network must be a type and model approved by the Head of IT or the Technical Service Manager.
- Mobile phones must have a current and supported operating system installed.
- All devices will be centrally managed under the approved Mobile Device Management (MDM) platform.
- IT may adjust the MDM security profile deployed to devices, without warning, to suit the current risk appetite of the institute.
- Lost devices must be remotely wiped, and the connection cancelled/barred.
- The device must be returned to the IT team, upon request, for maintenance and when the user ceases to provide services to Toi Ohomai or when it has been deemed the user no longer requires this service.
- Personal Apps: All app purchases made from online application stores (e.g. Apple's AppStore) for personal use are to be paid in full by the individual and remain under the ownership of the individual. Personal apps will not be supported by Toi Ohomai. It is the user's responsibility to back up the information stored in personal apps.
- Official Apps: All app purchases for Toi Ohomai use must be processed by IT and managed through MDM. Toi Ohomai must ensure there is a method to backup and remotely wipe data stored in Toi Ohomai official applications.
- Personal apps may be removed from corporate devices if they are believed to impede device performance, stability, or security.

- Users must discuss their requirements with IT Support before they travel overseas, otherwise costs may be recovered from the individual.
- The contact details of employees/contractors/volunteers including phone numbers and email addresses are published for internal use only. They are not to be distributed to third parties, published on the Internet without the authorisation of an Executive Leadership Team member.
- Divert destination recipients must agree to be the recipient for calls.
- To prevent the risk of falling victim to overseas toll fraud, International numbers are blocked by default from desk phones. The IT team will lift this restriction on a phone-by-phone basis temporarily or permanently upon request by the budget holder.

4.11.2 Devices that do not belong to Toi Ohomai – BYOD and contractor owned

- Devices not managed by Toi Ohomai may not be connected to any part of the Toi Ohomai environment or institutional networks (except for Guest wi-fi).
- Staff personal devices must use the GUEST network which attributes traffic to the device holder.
- Toi Ohomai's applications and data are to be separated from personal applications and data. Pre-approved technologies for this include: Thin Client (Terminal Services/Citrix/etc) or web-based applications.
- The Toi Ohomai security profile(s) (for example: Exchange Client Policies, MDM, Group Policy) will be enforced on the devices connecting to or synchronising with Toi Ohomai's computer systems and services.
- Toi Ohomai's data will be remotely wiped if the device is lost/stolen.
- Toi Ohomai's data will be remotely wiped when the user no longer provides services to Toi Ohomai.
- Toi Ohomai must be informed without delay if a BYOD/Contractor Owned Device is lost or stolen.
- Maintenance responsibilities for non-Toi Ohomai owned devices are the responsibility of the device owner.
- Unless covered by other policies or agreements, no costs associated with the use of a non-Toi Ohomai device will be reimbursed by Toi Ohomai.

4.12 Wireless access control

Toi Ohomai will securely use wireless local area networks (WLANs), access points, and wireless client systems.

- An inventory of authorised wireless access points connected to the wired network will be maintained.

- Advanced Encryption Standard (AES) encryption will be used to encrypt wireless data in transit.
- Wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)] will be disabled unless such access is required for a business purpose.
- A separate wireless network will be created for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.

5 CRYPTOGRAPHY

When used correctly, cryptography can protect confidentiality, authenticity and integrity of information. A clear policy on the use of cryptography, coupled with sound implementation of cryptographic systems, helps to ensure that information is properly protected.

5.1 Encryption Requirements

- [] Institutional and Sensitive information must be encrypted in transit across open, shared, unencrypted or public networks using TLS v1.2 or IPSEC.
- [] Sensitive information must be encrypted at rest (whilst stored on disk) using AES-256. This should be implemented in hardware or in the OS to provide a seamless experience to the user.

5.2 Public Key Infrastructure (PKI)

5.2.1 General principles

- Internal certificates must not be used to secure services for devices that cannot have the Toi Ohomai trusted root certificate installed.
- All public facing cryptography must use a certificate signed by a public trusted certificate authority.
- All certificates will be issued as RSA2048 and SHA256 (minimum).
- Toi Ohomai's IT team will maintain a list of internal and external certificates, including the certificate name, issuer, issue date, expiration date and services that depend on the certificate.
- Certificate lifecycles will be proactively managed, so certificates are renewed before they expire.
- All core PKI processes (Issue, Renew, Revoke, etc) are to be fully documented.
- All PKI private keys and administrative systems are to be classified as Sensitive.

5.2.2 External (Public) Certificates

- The private key for wildcard certificates will be held on a USB drive and stored in a secure location (see definition below).

- Certificates provided to third party hosts must only be for the specific (sub-)domain they host. No external/third party must ever be given a Toi Ohomai wildcard certificate.
- Public certificates will be valid for 1 year

5.2.3 Internal Certificates

- The Toi Ohomai root certificate authority (CA) must:
  - Be physically disconnected from all network connectivity.
  - Have all unnecessary services, accounts, ports and connectivity disabled.
  - Have a single local account for issuing certificates and administering the server.
  - Have a single local account for reviewing audit logs.
  - Have a local auditing policy to record all CA service events.
  - Use AES hard drive encryption using TPM (e.g. Bitlocker).
- The root CA server is exempt from the Patching and Vulnerability Management standard.
- Any updates required must be performed manually using an offline version of the update files.
- Internal certificates will be valid for:
  - Root CA: 20 Years
  - Subordinate (issuing) CA's: 10 Years
  - Issues/Auto-enrolled Certificates: 1 Year
- Certificate revocation lists will be published to internal, high-availability, webservers.
- Private keys from the root CA will be held on a USB drive and stored in a secure location.
- The root CA server is to be backed up immediately before and after each change. The backup is to be held on USB key within a secure location.

5.2.4 Secure Location

- The "secure location" referenced in this standard is to be:
  - Environmentally friendly to USB media.
  - A separate location to the primary data (server/keys).
  - Physically secured to only those who are specifically authorised for access.

6 PHYSICAL AND ENVIRONMENTAL SECURITY

Physical security is the first defence to prevent unauthorised access, damage and interference with the organisation's information and information processing facilities. Proper physical security reduces the risk of loss, damage, theft or compromise of assets and interruption to operations.

- [] Access to sensitive areas, for example server rooms or switch cabinets, must be limited to specific people who need the access to perform their duty. Their access must be properly authorised by the Technical Service Manager or a delegate.
- [] Prior to gaining access to any non-public areas, third parties must either Sign-in at the reception desk or be accompanied by a staff member.
- Whilst working in a non-public area, staff and third parties may be monitored by Toi Ohomai employees using (but not limited to); CCTV, Server Session Recording, Console Logging.
- Identification badges, physical access cards or computer authentication tokens that have been lost or stolen (or are suspected of being lost or stolen), must be reported to the IT team immediately so that their access can be revoked.
- [] Portable devices (e.g. USB sticks) must not be used to store information unless an approved encryption technology is used and the device is securely erased by IT staff after use.
- [] If a storage device containing Toi Ohomai information is lost then this should be reported to the Head of IT and Business Owner immediately.
- Toi Ohomai must be informed without delay if a Toi Ohomai device is lost or stolen.

7 COMMUNICATIONS AND OPERATIONS MANAGEMENT

Operational information security is achieved through careful management and reporting as well as the technical configuration management for server operating systems, appliances, switches, firewalls and software. The IT department is responsible for the operational security of the applications and infrastructure.

A disciplined focus on, and awareness of, operational security requirements build an information security culture and helps to ensure that security is a consideration in all aspects of the IT lifecycle.

7.1 Operational support and maintenance requirements

- All users of Toi Ohomai's IT platforms must have undertaken an approved IT Induction.
- Incidents, outages, and service requests must be reported through the IT team and must be logged and maintained in the approved ticketing tool.
- Toi Ohomai systems/websites must include advice for users to follow to report problems that may indicate a security issue. This should be directed to IT support.
- All production systems must be actively monitored for service degradation or indicators of security compromise.

- All production systems must be maintained in accordance with the supplier's recommendations.
- All requirements imposed by insurance policies must be met.
- All software and hardware in production must be under a support agreement with either:
    - the vendor
    - an approved partner, or
    - internally (where vendor/partner support is not available).
- Repairs and servicing of equipment must be performed only by qualified and authorised technical personnel and, if the equipment is taken off site for repair, it should be inspected and checked in a test environment prior to being reconnected to the production network to ensure it operates as expected and has not been tampered with.
- Any device being sent off-site for repair must be securely erased.
- Critical hardware must be fitted with surge protection equipment and protected from power outages by a UPS.
- All cabinets and equipment must be earthed in accordance with the manufacturer's requirements.
- Hardware critical to the provision of business services must be sited or protected to reduce the risks from environmental threats, hazards, opportunities for unauthorised access and risks to health and safety.
- All software licenses, registrations and other formal agreements featuring a Name field must use the institute's name or relevant department whenever possible.
- All publicly discoverable records relating to the ownership of assets (including Domain name WhoIs records) must reference Toi Ohomai and the IT team. Individual staff names must not be used.
- [] Sensitive systems must present an approved legal banner before accessing the system (where this is supported by the platform).

7.2 Secure Configuration for Hardware and Software

Toi Ohomai will establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.

- Security configuration standards (baselines) will be documented for all authorised operating systems and software.

- Secure images or templates will be maintained for all systems in the organisation based on the organisation's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
- All new implementations of a product or major upgrades must be implemented using an approved hardening standard (baseline).
- New implementations of a product will use the same baseline as has already been used for other implementations of the same product, so long as the baseline is fit for purpose. Fit for purpose considerations include (but are not limited to):
    - Is the product being used for substantially the same task?
    - Is the product operating in the same risk environment? See (Classifications)
    - Is the configuration valid for the version of the product being deployed? (e.g. newer versions may not accept older setting, or newer versions may introduce additional protections which should be configured).
- Where no baseline exists, or the incumbent baseline is not fit-for-purpose, the implementer will determine a viable alternative with preference shown for (in order of preference):
    - Vendor recommended baselines.
    - CIS baseline.
    - Industry/Environment specific baselines from a recognised/respected authority.
- Where no 3rd party baseline is identified the implementer must produce one for the product. To do this, they should review and document each configuration option in the product and apply their judgement based on the principles of:
    - Conform with Toi Ohomai policies and standards
    - When available, use settings from another baseline to maintain consistency.
    - Use industry good practice.
- Any new configuration baselines generated will be reviewed by the Toi Ohomai's ITSF before being stored in the approved repository.

7.3 Email and Web Browser Protections

Toi Ohomai will minimise the attack surface and the opportunities for attackers to manipulate human behaviour though their interaction with web browsers and email systems.

- Only fully supported web browsers and email clients will be used, ideally only using the latest version.

- Unauthorised browser or email client plugins or add-ons will be disabled or uninstalled.
- Network-based URL filters will be configured to limit the ability to connect to websites not approved by the organisation. This filtering shall be enforced for each of the organisation's systems, including, where possible, whether devices are physically at Toi Ohomai's facilities or not.
- URL-categorisation services will be used to ensure that categories are up to date with the most recent website category definitions available. Uncategorised sites will be blocked by default.
- All URL requests from each of the organisation's systems will be logged where possible to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.
- Only approved DNS servers will be used, and Domain Name System (DNS) filtering services will be used to help block access to known malicious domains.
- To lower the chance of spoofed or modified emails from valid domains, Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification should be implemented starting with the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.
- Email attachments will be blocked at the email gateway if the file types are unnecessary for the organisation's business.

7.4 Limitation and Control of Network Ports, Protocols, and Services

Toi Ohomai will manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices to minimise windows of vulnerability available to attackers.

- Only network ports, protocols, and services listening on a system with validated business needs should be running on each system.
- Host-based firewalls or port-filtering tools will be configured on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
- Application firewalls will be placed in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

7.5 Patching and vulnerability management

Toi Ohomai will continuously acquire, assess, and act on new information to identify vulnerabilities, remediate, and minimise the window of opportunity for attackers.

7.5.1 Vulnerability Management

- A vulnerability scanning tool will be used to automatically scan all systems on the network on a regular basis to identify all potential vulnerabilities on the institute's systems.
- Authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested will be undertaken.
- The results from consecutive vulnerability scans will be regularly compared to verify that vulnerabilities have been remediated in a timely manner.
- A risk rating process should be used to prioritise the remediation of discovered vulnerabilities.

7.5.2 Patching

- Automated tools will be used to patch operating systems and application software.
- Critical and security patches will be installed within 30 days of their release.
- A process will be implemented to evaluate patches for criticality and relevance.
- Where possible, patches will be successfully tested on non-production systems or less critical systems prior to being loaded on production and critical systems.
- Successful backups of critical systems will be verified prior to installation of patches and a mechanism for reverting to the patch levels in effect prior to patching will be identified.
- Patches will be applied during agreed maintenance windows in cases where the patch application will cause a service interruption for critical systems.
- Post upgrade checks to confirm patch success and service availability will be undertaken for critical systems and services.

Exceptions

- Patches to fix issues which Toi Ohomai is not vulnerable to need not be applied.
- Non-critical, non-security patches and feature updates and patches may be installed to suit Toi Ohomai's requirements and in step with regular maintenance processes. There is no mandate to install non-critical/non-security patches within a specific timeframe.
- The Head of IT or Technical Service Manager may, on a case-by-case basis, instruct the immediate deployment of critical patches where the vulnerability being patched represent a serious and immediate risk to Toi Ohomai.
- Exceptions to this standard require formal approval from the Head of IT.

7.6 End point protection

Toi Ohomai will aim to control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action.

- Centrally managed anti-malware software will be used to continuously monitor and defend each of the organisation's workstations and servers.
- The anti-malware software will regularly update its scanning engine and signature database.
- Anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or as separate tools should be deployed where possible to apply protection to a broader set of applications and executables.
- Devices will be configured so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
- Devices will be configured not to auto-run content from removable media.
- All malware detection events will be sent to enterprise anti-malware administration tools and event log servers for analysis and alerting.
- Domain Name System (DNS) query logging should be configured to detect hostname lookups for known malicious domains.
- Content received from an external source (e.g. email or FTP) must pass through Toi Ohomai's approved malware detection and protection services.
- Material containing viruses must be permanently deleted from all systems (including archives/backups).

7.7 Secure Configuration for Network Devices

Toi Ohomai will establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure.

- All configuration rules that allow traffic to flow through network devices should be documented, including the specific business reason for each rule, a specific individual's name responsible for that rule/ business need.
- Network devices will be regularly updated with the latest stable version of any security-related updates.
- Network devices will be managed using multi-factor authentication and encrypted sessions wherever possible.

7.8 Boundary Defence

Toi Ohomai will detect/prevent/correct the flow of information transferring networks of different trust levels.

- Network diagrams/inventory showing all the organisation's network boundaries will be maintained.
- Firewall rules must be reviewed annually.
- Firewalls should Deny by default and have explicit Permit rules for approved services.
- Communication from known malicious or unused Internet IP addresses will be denied and access will be limited to trusted and necessary IP address ranges at each of the organisation's network boundaries.
- Unknown or unauthorised TCP or UDP traffic and applications will be denied ensuring that only authorised protocols and applications can cross the network boundary in or out of the network at each of the organisation's network boundaries.
- The principle of least privilege should be applied where traffic from a low trust zone passes into a higher trust zone. For example, Internet to DMZ, DMZ to Corporate.
- All traffic traversing network boundaries will be logged.
- Network-based Intrusion Detection Systems (IDS) sensors will be deployed to look for unusual attack mechanisms and detect compromise of these systems at each of the organisation's network boundaries.
- Network-based Intrusion Prevention Systems (IPS) will be deployed to block malicious network traffic at each of the organisation's network boundaries.
- All network traffic to or from the Internet passes through an authenticated application aware firewall or proxy that is configured to filter unauthorised connections.
- Traffic at the network boundary to the internet that is encrypted will be decrypted enabling content inspection. However, the organisation may use Allowlists of permitted sites that can be accessed without decrypting the traffic.
- All remote access to the organisation's network must encrypt data in transit and use multi-factor authentication.
- An approved web application firewall should be placed in front of all Toi Ohomai owned/operated webpage/API endpoints.
- All websites and APIs must be suitably rate limited to reduce the impact of accidental or deliberate misuse.

7.9 Email security

- Email must pass through one or more SMTP antivirus and antispam systems before being accepted into the SMTP servers/services.
- The system must block attachments with executable files or file types known to commonly contain malware. Blocked attachments must require the review/approval of the IT team for release.

- The email system will automatically attach a disclaimer to all outbound email to ensure the recipient is aware of the context and limitations of the email content.
- All email servers or services used to send messages on behalf of an official Toi Ohomai domain name will be configured with DKIM and SPF records.
- ] Sensitive information, being sent to an external party by email, must be encrypted with AES256 encryption.

7.10 Network Management

- Toi Ohomai must maintain a current inventory and diagram of all connection points and data flows for computer networks owned and managed by Toi Ohomai including approved wireless networks and external access points. A copy of which must be part of the Disaster Recovery documentation.
- Network address schemes should be logical and conform to the relevant inter-organisation IP Addressing agreements.
- Externally facing DNS servers must not support recursive DNS queries.
- Externally facing DNS servers must not reveal private/internal IP ranges.
- DNS must only be permitted from trusted devices to trusted DNS servers.
- Internal DNS servers must recurse to either the ISP allocated server(s) or Quad9.
- Devices which do not meet the security criteria for joining a network must be actively blocked.
- Clear-text protocols (e.g. Telnet, SNMPv1/2) must never be enabled where a secure solution (e.g. SSH, SNMPv3) is available.

7.11 Data Recovery Capabilities

Toi Ohomai will deploy and test processes and tools to properly back up critical information ensuring a proven methodology for timely recovery of it.

- All system data must be automatically backed up on a regular basis.
- All the organisation's key systems must be backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
- Backups should be tested regularly by restoring from backup media.
- Backups must be properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
- All critical backups should have at least one offline (i.e., not accessible via a network connection) backup destination.

7.12 Destruction, sale or transfer of equipment

- When equipment reaches the end of service it must be securely erased (using the method prescribed in this policy) and any Toi Ohomai identification removed (e.g. Asset tags).
- Where equipment is to be sold or gifted, a legally robust written agreement should be in place to absolve Toi Ohomai of any legal or reputational blame for broken equipment or damages.
- [] All devices used to hold Toi Ohomai Corporate material must be securely erased using multi-pass sanitisation software, or physical destruction.
- [] All devices used to hold Sensitive information must be securely shredded by a professional destruction company.
- [] A certificate of destruction must be provided by the destruction company and is to be retained by Toi Ohomai for 2 years.

8 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Considering the security aspects and requirements of systems at each step in their lifecycle is a key ingredient to ensuring that systems will have the security attributes required operationally.

Ensuring that security requirements are clearly defined early in any acquisition or development effort, helps to prevent costly mistakes and avoids live applications with a poor security posture. It is also important to properly protect test data – test data is often "real" information.

- Toi Ohomai employees or contractors must not undertake the purchase of any technology or information products or services without consulting the Head of IT.

8.1 Cloud Computing

- All new cloud service use requires the approval of the Head of IT.
- The business owner of the cloud computing service must complete a *Cloud Assessment Form* to ensure that:
    - The cloud service is compatible with Toi Ohomai information and devices.
    - The service provides the reliability/up-time required by the business.
    - The cloud service has the capacity and functionality for the expected deliverable.
    - The cloud service geographic location delivers Toi Ohomai's expectation of system performance and security.
    - Information on the service is added to the DR documentation.
    - Contracts and service agreements have been reviewed.

- Costs are understood and budgeted for.
- Integration issues are identified.
- Authentication and account maintenance mechanisms are identified
- Product ownership and support is clear.
- Risks are identified and mitigated to an acceptable level.
- Training is identified.
- Data classification has been established and is compatible with the service.
- There is an acceptable contractual obligation for the cloud provider to return data to the organisation when the organisation wishes to terminate the cloud service.

- The business owner of the cloud computing service must regularly monitor and review the services, reports and records provided by the cloud service provider and must conduct a regular audit of the cloud service provider's performance in accordance with the Service Agreement.
- The business owner of the data being stored/processed in the cloud must satisfy themselves that the cloud service is suitable for the classification of data being stored or processed by the service.
- [] Public information may be stored/processed in any cloud service.
- [] Corporate and Sensitive information may only be stored in cloud services approved for that classification.

8.2 Software Development

Toi Ohomai will manage the security life cycle of all in-house developed and acquired software to prevent, detect, and correct security weaknesses.

- Secure coding practices appropriate to the programming language and development environment being used must be established and used.
- For in-house developed software, explicit error checking should be performed and documented for all input, including for size, data type, and acceptable ranges or formats.
- All software acquired from outside the organisation should be supported by the developer or appropriately hardened based on developer security recommendations.
- Only standardised, currently accepted, and extensively reviewed encryption algorithms may be used.
- All software development personnel should receive training in writing secure code for their specific development environment and responsibilities.
- Static and dynamic analysis tools should be used to verify that secure coding practices are being adhered to for internally developed software.

- A process to accept and address reports of software vulnerabilities should be established, including providing a means for external entities to contact your security staff.
- Separate environments for production and non-production systems should be maintained.
- Developers should not have unmonitored access to production environments.
- Web applications should be protected by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.
- For applications that rely on a database, standard hardening configuration templates should be used. All systems that are part of critical business processes should also be tested.
- Public facing software/services must be security tested before being placed into production.
- Where software development is outsourced the institution must ensure that one or more of the following requirements are met:
  - The source code is provided to Toi Ohomai.
  - The appropriate right-of-use agreement(s) are issued.
  - Escrow arrangements are put in place.
- Source code must be stored securely in an approved source code repository.
- Application must not be built with trap doors or Easter eggs.
- Debug information and functionality must be disabled in production.
- Error reporting must be reported to an appropriate internal role (e.g. IT team, Development team, etc).
- Websites must be tested against the OWASP Top 10 cybersecurity controls. Where the vendor is unable to do this, or Toi Ohomai wishes to increase assurance, a third-party can be contracted to perform this test.
- Third party frameworks/libraries must be copied to and referenced from a Toi Ohomai controlled server.
- Frameworks/libraries must be fully patched at the time of deployment.
- Error reporting functionality which sends to an external party must be disabled.
- Public facing systems must use industry standard mechanisms or a web application firewall for rate limiting to negate brute force attacks.

8.3 Change management

- Toi Ohomai will operate a Change Advisory Board (CAB)
- Changes will be subject to CAB approval where:
  - The change could result in a Toi Ohomai asset becoming unavailable, unresponsive or falling below agreed service levels.
  - There is a risk that the change could affect something outside the scope of the asset being changed.
  - Other business units or roles may need to know about the change or schedule it around their own changes.
  - The nature of the change requires recording to ensure the reasons for the change and the process to reverse it are captured.
- The following are out of scope for change management and CAB:
  - Any system function or data entry that can be performed by a standard user.
  - Systems that are not in production (Provisioning, Test, Dev, etc).
  - Power-cycling (resetting) a failed device, or a passive member of an HA cluster.
- A formal change management process will be followed where a change is being made to any Toi Ohomai technology/information asset. This includes (but is not limited to) the servers, workstations, devices, databases, updating of firmware on network devices, and software used in the Toi Ohomai's network.
- No changes will take place without an approved Request for Change (RFC).
- RFC(s) will be logged for each change. The change request passes through four phases:
  - Initiation - where the Request for Change (RFC) is logged by the Change Owner.
  - Approval - where the change is reviewed and voted on by the Change Advisory Board (CAB).
  - Implementation - where the change is made.
  - Closure/Rollback - once verification is complete.
- For a complex change that may have significant impact or security implications, the Change Owner or Project Manager should initiate the change before significant work is undertaken. This maybe done as part of the *Toi Ohomai Project Framework*. This will help to ensure that security implications are well understood before the development phase and that expectations can be clearly set before too much investment in a change is made.
- Changes will be categorised as:
  - **Normal:** An RFC which follows the full Change Management Process.

- **Pre-Approved/Standard:** A regular, templated, change which has been thoroughly reviewed and approved by the CAB as being low-risk and having a robust easy to repeat process. Once approved by CAB, pre-approved changes are recorded on the "Pre-Approved Change Register". Pre-approved changes bypass the CAB Approval stages. Regular patching is an example of a pre-approved change.
- **Emergency:** A change intended to repair a service disruption or imminent threat of service disruption. Approval may be verbally given by the CAB Change Manager, the Head of IT, or the Executive Leadership Team member responsible for the asset. The change may be recorded after the event. Emergency changes are never to be used to bypass the "Normal" change process due to a lack of planning or preparation.

- A Change Advisory Board (CAB) will review and approve all Request for Change (RFCs). There may be different CABs for different environments or types of change.
- The Change Advisory Board(s) will be led by a Change Manager who is responsible for controlling the change process, ensuring CAB participants vote in a timely way and hold people to account for changes made outside the process.
- The Change Manager decides what roles/individuals are members of the CAB. This may be varied on a change-by-change basis to involve subject matter experts or remove CAB members who are not relevant to the RFC.
- CAB members may vote in three ways**: Approve, Abstain, Reject.**
  - A change may not proceed with any Reject votes.
  - A CAB member may change their vote.
  - A CAB member may nominate a proxy when they will be temporarily unable to fulfil their CAB obligations through sick or annual leave.
  - CAB members who do not vote within 5 working days of the RFC being logged will be considered to have Abstained.
  - Votes must be recorded using the approved Change Management tool (this may include email).
  - Where any member of the CAB feels there is insufficient detail in the RFC to vote, or they feel inclined to "Reject" the RFC, then the Change Owner should be given the opportunity to refine the RFC, or to attend a CAB meeting to discuss the change.
  - CAB members who do not feel capable (through a lack of relevant skill/knowledge) to make a judgement call must abstain without delay.
  - RFC change windows must include the time required for testing and (if required) rollback of the change.
  - The Change Owner may vote on their own RFC where they are also a member of the CAB.

- External parties performing changes will provide the RFC details to a Toi Ohomai point of contact who will be the Change Owner.
- A Request for Change (RFC) will contain the following fields. Some fields may be left blank depending on the nature of the change.
  - RFC number.
  - The change owner name and contact details.
  - The date and details of the CAB approval.
  - Change title and description.
  - Start date and time of the change window.
  - End date and time of the change window.
  - Category of change (Normal, Pre-approved, Emergency).
  - Expected/potential Impact.
  - Communications plan.
  - System(s) affected
  - Service(s) affected
  - Peer reviewer and peer review completion
  - Change plan (detailed step-by-step technical change).
  - Potential risks and mitigations.
  - Test plan.
  - Rollback plan.

9 HUMAN RESOURCES SECURITY

Sound security practices surrounding the HR practices should ensure that potential employees and contractors are suitable for the roles which they will hold, that employees are aware of and fulfil their security obligations and, that the organisation's interests are protected after an employee leaves the organisation.

9.1 Prior to employment

Toi Ohomai must ensure staff, contractors and third-party users understand their responsibilities, are suitable for the roles they are considered for, and are screened to reduce the risk of theft, fraud or misuse of Toi Ohomai data and systems. This requires (at minimum) the following:

- Providing a position description for all positions within the organisation.
- Ensuring that information security responsibilities are defined for all employees (in position descriptions or policies).
- References and qualifications are checked.

9.2 Security Awareness and Training Program

Toi Ohomai will, for all functional roles in the organisation, ensure that sufficient awareness is maintained to protect the organisation's systems and information.

- A security awareness program for all workforce members to complete on a regular basis must be created to ensure they understand and exhibit the necessary behaviours and skills to help ensure the security of the organisation. The organization's security awareness program should be communicated in a continuous and engaging manner.
- Users must be trained on the importance of enabling and using secure authentication.
- Users must be trained how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.
- Users must be trained how to identify and properly store, transfer, archive, and destroy sensitive information.
- Users must be trained to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
- Users must be trained to be able to identify the most common indicators of an incident and be able to report such an incident.

9.3 Termination or change of employment

Toi Ohomai's responsibilities include ensuring an employee's, contractor's or third-party user's exit is managed - and that the return of all equipment and the removal of all access rights are completed.

Additionally, employees should be reminded that any confidentiality requirements endure beyond the term of employment.

10 SUPPLIER RELATIONSHIPS

Supplier relationships need to be managed to help successful security outcomes. Specifically, assets which are accessible to suppliers need to be appropriately protected and supplier agreements should provide for clearly agreed security practices.

- Suppliers must be formally made aware of Toi Ohomai's security policies, standards and guidelines as part of contract negotiation and onboarding.
- Suppliers should be compelled to comply with these via the commercial arrangements put in place.
- A formal acknowledgement of Toi Ohomai's policies and standards and a clear agreement outlining the expectations is included at Appendix 1 of this document.

11 INCIDENT MANAGEMENT

Toi Ohomai will protect its information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

- Incident response plans should be written that define roles of personnel as well as phases of incident handling/management.
- Management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles should be clearly designated.
- Third-party contact information should be assembled and maintained to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors and partners.
- Information should be published for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.
- Incident response exercises and scenarios should be planned and conducted for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.
- Notification of Cybersecurity threats (such as CERT NZ announcements, spikes in Phishing, etc) must only be disseminated internally or externally by IT team or the Technical Service Manager.
- Toi Ohomai systems/websites must include advice for users to follow to report problems that may indicate a security issue. This should be directed to IT Support.

12 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

In the event of system disruption or compromise, it is essential that plans are in place to restore key system and data stores and resume business operations. This business continuity plan should include those activities and considerations necessary to protect sensitive Toi Ohomai information during this process.

- Business Continuity Management for Toi Ohomai is a responsibility of the Leadership Team. Refer to the Toi Ohomai Business Continuity Plan (BCP) for more information.

  Note: A “Business Continuity Plan(s)” is the plan for how the organisation’s teams will continue to deliver their critical services whilst key systems are unavailable. This may include details such as alternative sites, paper-based processes, backup systems and equipment.
- ICT Disaster Recovery ICT Disaster Recovery (DR) planning is a responsibility of the Head of IT.

Note: The "Disaster Recovery Plan" is a document or documents which contain technical information which will assist with the rebuilding of an asset (e.g. as-built document, credentials, configuration files, key vendors contact details, license keys, etc).

- A Disaster Recovery Plan (DR plan) will be established and maintained.
- Sensitive information protection requirements must be maintained in a DR situation.
- Business critical services must be provisioned in a high availability (HA) configuration (active-active or active-passive) to remove the risk of a single point of failure.
- Disaster Recovery documentation must contain adequate information and make suitable provision to restore services within the timeframes stated in the Business Continuity Plan.
- Disaster Recovery documentation must be reviewed and updated every 12 months.
- Disaster Recovery documentation and all supporting information must be kept in a secure location where it can be accessed in the event of an emergency. Copies must be in Tauranga and Rotorua.
- Disaster Recovery plans should be tested at least annually.
- A real event may be used as a DR test where it gives assurance that the DR plan is operating correctly and is retrospectively documented as test.
- All deficiencies identified in the DR plan must be remedied within 3 months.
- DR test reports must be submitted to the TSF detailing the scope of the test, results of the test and deficiencies identified.
- Backups of essential business information and software must be stored in a secure room which is environmentally friendly to media. Access to backup media is limited to approved staff.
- Backups must not reside in the same physical location as the primary source.
- The backup media must be of sufficient quality to guarantee reliability beyond the legal/policy data retention period of the information it holds.
- Appropriate equipment to mount recovery media must be retained and maintained.
- Used backup media that is no longer required must be shredded and a certificate of destruction kept for 2 years.

13 COMPLIANCE

13.1 Inspection and management

- The institute maintains the right to conduct inspections of any equipment or service that it owns or manages without prior notice to the user or custodian.

- Managers and supervisors are responsible for their direct reports' use of Toi Ohomai's systems and equipment and should be alert for any activity that could indicate misuse or inappropriate use of Toi Ohomai's resources.
- Managers and supervisors must, upon request for the Head of IT, review their staff/contractor/volunteer's use of Toi Ohomai equipment to ensure it is being used in a way that is consistent with the institute's policies, standards, procedures and guidelines.
- Equipment must be used in a way that does not void manufacturer or vendor warranties.
- Any material that IT believes may be in breach of copyright may be removed without notice.
- All licensed IT products must be proactively managed to ensure license compliance is always maintained.

13.2 Logging and Alerting Policy

Toi Ohomai will collect, manage, and analyse audit logs of events that could help detect, understand, or recover from, an attack.

- Two synchronised time sources will be used from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
- Toi Ohomai captures log information from all network device, servers, applications, cloud services and management devices in off-device repositories. This information is available to authorised Toi Ohomai staff for fault finding and security incident analysis.
- Non-networked devices (standalone devices) are exempt from this policy due to the practical limitations of the device. If applicable, the policy below should be used as a guideline for configuring the device's on-device logging.

13.2.1 Event Types and Sources

- Events must be logged by all Toi Ohomai administered IT systems. Including (but not limited to), network devices, servers, cloud services, applications, control units, UPSs.
- Environments operated by third parties (such as Cloud software-as-a-service) must (where possible) be configured to expose the "High" importance events to the approved logging platform.
- The following event types must be collected and retained for the periods indicated (subject to the capabilities of the devices).

Event/Log Type	Importance	Retention
Security Events e.g. • Login attempts. • Logouts. • Password change attempts. • Account creation, modification or removal. • Security group creation, modification or removal. • Failed attempt to elevate privileges. • Creation, modification or deletion of sensitive files or folders.	High	24 months
Administration Events e.g. • Configuration changes. • Configuration capture. • Firmware upgrades. • Traffic capture, observe or mirror commands.	High	24 months
High-Priority System/Application Events e.g. • Warning, Error or Critical priority events. • Security related events/failures. • System start-up and shutdown. • Service/process starting and stopping. • Installation and removal of software. • System recovery activities. • Database data import/export. • Database schema changes.	High	24 months
Routine System/Application Events e.g. • Info priority events. • DNS queries. • Webserver requests. • Backup and archival events.	Medium	6 months
Diagnostic/Performance Events	Low	6 weeks

e.g. • Firewall processing logs. • Debug logs.		

- Log records must include:
    - Timestamp of the event (in UTC).
    - The user/process associated with the event.
    - The action or type of event and any relevant data (event description).
    - Success or failure of the event.
    - Identifier of the system/application that generated the event (event source).
    - Remote address (if the event occurs over a network connection).
- Adequate storage space will be provisioned to ensure that all systems that store logs have space for the logs generated.
- Retention and disposal must occur automatically in line with the retention periods.

13.2.2 Centralised Logging Platform

- Devices must transmit their events in real-time to the approved centralised logging platform.
- The approved platform(s) must collect, store, collate and offer query functionality for the event data.
- A consistent NTP master time source must be used across all devices and the logging platform.

13.2.3 Data Security

- Event data must be stored in dedicated storage only accessible to the logging platform servers.
- Access to the logging platform and its underlying datasets must be restricted to Toi Ohomai staff with a genuine need-to-know on a named user basis.
- Other than through automated retention and disposal processes, log entries must not be removable or modifiable by any user or administrator.
- If the platform requires a super-admin account, which offers the ability to remove or modify records, then the password is to be stored and protected in line with the Identity and Access Management (IAM) Policy (Privileged Accounts section).
- Where possible, passwords, tokens, and other sensitive information must be masked/redacted from logs before storage.

- Where possible, log information must be encrypted in transit to ensure log integrity and provide confidentiality to information which has yet to be masked.
- Choice of log method/format (syslog, agent, SNMP, etc) must be made based on the features of the source device, features of the log platform and the security principles of (in high to low priority order) availability, integrity, and confidentiality.

13.2.4 Alerting

- The logging platform must run checks to notify the IT team via email or SMS for the following classes of event:
    - Successful or unsuccessful generic privileged account logins (e.g. Administrator, Root).
    - Successful or unsuccessful login attempts through console ports.
    - High-risk failed logins:
    - DMZ: 3 failed access attempts (or an account lockout) over a period of 15 minutes, to any account.
    - Corporate: 3 failed access attempts (or an account lockout) over a period of 15 minutes, to any privileged account.
    - Successful or unsuccessful traffic flow captures.
    - A new, modified or deleted privileged account.
    - Changes to the logging platform configuration that would affect data storage/retention.
- Processing time for an event logged to an email alert being sent, must be under 5 minutes.
- All alert emails must include at least one generic mailbox/mailing list which is continuously monitored.
- Standard operating procedures must be available to the recipients of email alerts to inform a consistent, appropriate, and timely response.

13.3 External Audit

- Every 3 years a comprehensive cybersecurity technical audit of the computer systems and networks owned or managed by Toi Ohomai must be conducted by an independent auditor. The report resulting from this project must include a detailed description of the security risks currently facing the organisation and recommendations for preventing or mitigating these risks

13.4 Penetration Tests

- Penetration testing should be conducted when new internal or external information systems and services are commissioned, or when significant change to existing systems is undertaken.
- Regular external and internal vulnerability scans should be used to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.
- Use vulnerability scanning tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.
- Penetration tests must be approved by the Head of IT

APPENDIX 1: SUPPLIER CYBERSECURITY AGREEMENT

Last Updated: March 2021

This policy applies to all suppliers to Toi Ohomai who have access to Toi Ohomai's **data**/**systems** or are storing/processing data for which Toi Ohomai is legally responsible.

Suppliers are required to abide by all the relevant requirements of the Information and Technology Policy.

DEFINITIONS

- **Reasonable steps** mean the skill, diligence, care, and foresight expected of a highly skilled and experienced person in the same or similar circumstances.
- **Security incident** means the unauthorised access, use, alteration or destruction of any Toi Ohomai **data** or **systems**, or other compromises or breaches of your or our electronic or physical security.
- **Security vulnerability** means a weakness at the network, operating system, database or application software level, or within associated functions (such as a physical vulnerability at the location where Toi Ohomai's **data** is stored), that could allow a **Security incident** to occur.
- **Classified information** means any Toi Ohomai **data** or **systems** which process or store information which holds a data classification of Sensitive.
- **Data** means all data, information, text, drawings and other materials in any form that Toi Ohomai provides to you, or that you generate, collect, process, hold, store or transmit in connection with an Agreement, excluding Your Materials.
- **System** means an electronic information system, including (but not limited to) hardware, software and communications networks.
- **we**, **us** and **our** means Toi Ohomai.
- **Your materials** mean all software, documents and other materials created or owned by you or a third party independent of an Agreement, which are provided to Toi Ohomai by you or on your behalf.
- **Defence in depth** is a concept in which multiple layers of security controls (defence) are placed throughout an information technology (IT) **system**. Its intent is to provide redundancy in the event a security control fails, or a vulnerability is exploited that can cover aspects of personnel, procedural, technical, and physical security for the duration of the system's life cycle.
- **Least privilege** means giving a user account or process only those privileges which are essential to perform its intended function.
- **Minimise attack surfaces** means the attack surface of a software environment is the sum of the different points (the "attack vectors") where an unauthorized user can try to enter data to or extract data from an environment.
- **Secure by design** means that **systems** have been built considering security from the initial design phase, rather than as an afterthought.

INFORMATION SECURITY

1. Toi Ohomai's data is confidential. You must not access, store or use Toi Ohomai's data except as required to perform your obligations under an Agreement. When that Agreement ends you must securely delete or destroy (or, if required by the Agreement, return) all Toi Ohomai's **data**, except to the extent that you need Toi Ohomai's **data** to perform obligations owed to us under another Agreement or to meet any regulatory obligations.

2. Where Toi Ohomai's **data** includes personal information (as defined in the Privacy Act 1993), you must hold and process that personal information in accordance with your obligations under the Privacy Act 1993.
3. Unless restricted by law, you must disclose to Toi Ohomai, without delay, any attempt made by a third party to access Toi Ohomai's **data** or **systems**, whether that be by a malicious party or as part of a legal or legislative process, and whether the attempt is granted or denied.

SECURITY REQUIREMENTS

4. As a minimum, Toi Ohomai requires you to take all **reasonable steps** to implement the security principles of:
    a. **Defence in depth**;
    b. **Least privilege**;
    c. **Minimise attack surfaces**; and
    d. **Secure by design**.
5. Take all **reasonable steps** to prevent unauthorised use of, or access to, Toi Ohomai's **data** and **systems**. This requirement applies whether the services are provided directly by you or a third party, and where the Services use an on-premise or cloud-based solution.
6. Take all **reasonable steps** to prevent the introduction of **security vulnerabilities** that could impact on Toi Ohomai's **data** or **systems**.
7. Regularly monitor **systems** and audit logs to verify the effectiveness of the technical, administrative, and physical controls used to protect Toi Ohomai's **data** and **systems**.
8. Promptly apply security measures and patches designed to address **security vulnerabilities** in accordance with the recommendation of the supplier of hardware or software.
9. Ensure your Authentication, Authorisation and Accounting practices *(e.g. Microsoft Active Directory)* ensure only authorised parties can, and have, accessed Toi Ohomai's **data** and **systems**.
10. Identity *(e.g. **system** logons)* must specifically identify an individual user or system service and be non-repudiatory.
11. Authentication *(e.g. Passwords and Multifactor Authentication)* must follow a recognised industry practice (such as NZ Information Security Manual (NZISM), or National Institute of Standards and Technology (NIST) Special Publication 800-63).

EMPLOYEE & SUPPLIER MANAGEMENT

12. Ensure that your employees have the right level of cybersecurity awareness required to carry out their roles and responsibilities.
13. Ensure your employees and suppliers are aware of their obligations under this policy.
14. Validate the capabilities and security practices of any suppliers you engage (such as hosting providers and managed service providers) that could impact on the confidentiality, integrity or availability of Toi Ohomai's **data** or **systems**. Ensure the supplier agreement is fully compatible with the obligations of this policy and any agreement.
15. Ensure you promptly alter or terminate access to Toi Ohomai's **data** and **systems** when an employee's role or employment status changes.

SECURITY INCIDENTS

16. If you become aware of a **security incident** that has or may significantly impact the delivery of any service, or may have compromised the confidentiality, integrity or availability of Toi Ohomai's **data** or **systems**, you must:
    a. Notify us within 24 hours of becoming aware of the **security incident**;
    b. Provide all information we reasonably request in relation to the incident, its manner

of introduction and the impact that the incident has had or is likely to have;

c. Provide regular status updates for the incident until resolved; and

d. Provide as soon as practicable, but in any event within 7 days following resolution of the incident, a written report including (1) the date the incident occurred; (2) the length of any outage; (3) a summary of the incident; (4) details such as individuals involved in any aspect of the incident handling, how/when the incident was detected, what was impacted, and any containment strategies; (5) the root cause of the incident; and (6) what corrective action was taken to prevent reoccurrence.

17. If Toi Ohomai determines, in its reasonable opinion, that additional measures are required to contain, respond to or remediate a **security incident** (including but not limited to a customer announcement, credit monitoring services or fraud insurance) you will undertake those remedial actions and you agree by entering into any supplier relationship with Toi Ohomai that you will bear the cost of any such remedial actions.

18. All communications relating to the exposure, or potential exposure, of Toi Ohomai's **data** or **systems** must be made by a Toi Ohomai appointed spokesperson.

SECURITY ASSURANCE

19. In order to meet our responsibilities to our stakeholders, we may request that you provide evidence and results of a recent security assessment covering the scope of your service delivery to Toi Ohomai.

20. Where no such assessment exists or the assessment is older than 3 years, Toi Ohomai may request you engage a mutually acceptable independent third-party to undertake such an assessment.

21. If a security assessment reveals that your processes do not meet the minimum standards required by this policy or reveals significant deficiencies that result in an unacceptable level of risk to Toi Ohomai's **data** or **systems** then you must promptly meet with us to discuss and agree appropriate corrective steps and apply those steps without delay.