INFORMATION AND COMMUNICATION TECHNOLOGY PROCEDURES

Category	Communications and ICT
Procedures Owner	Chief Technology Officer
Last review	15 September 2025
Next review	30 September 2026
Approved by	Vice-Chancellor
Effective date	2 February 2024

1. PURPOSE

To support the Information and Communication Technology Policy.

2. SCOPE

This procedure applies to all ICT Systems & Services owned or used by the University for teaching, learning, research, and administration, and to all employees, students, contractors and anyone else who may be granted access to such facilities from time to time.

3. DEFINITIONS

Availability: ensuring that authorised Users have access to Information and associated assets when required.

Confidentiality: ensuring that Information is accessible only to those authorised to have access.

Connect: to physically, or logically establish a Connection to the Network.

Commodity Services An ICT system or service provided by a commercial service provider to a large and diverse set of customers.

Data: Data and Information created or acquired from any source in any format.

Email: a Network service that enables messages to be sent and received over the Network using computers and hand-held devices such as mobile phones.

Endpoint: physical devices that Connect to and share Information with the Network.

ICT Systems & Services: encompasses all AUT’s ICT for the capture, storage, retrieval, processing, display, representation, organisation, management, security, transfer, and interchange of electronic Data and Information and includes, for the avoidance of doubt, all AUT’s hardware, software, applications and Internet facilities.

Information: all records, documents and Data whether computerised or not and all Software whether developed by the University or otherwise acquired, that is owned by the University or entrusted to it for any purpose or used in the course of or associated in any way with the University’s business.

Information Security: the measures taken by the University to protect the Confidentiality, Integrity and Availability of Information and to safeguard the Information technology and communication systems of the organisation.

Integrity: safeguarding the accuracy and completeness of Information and processing methods.

Internet: the Internet is a public global Network linking organisational Networks and Data sources around the world enabling them to exchange and share Information.

Intranet: the Intranet is a private local area Network (LAN) that uses the same technology as the Internet to link the internal Networks and computers of an organisation, enabling them to exchange and share Information. The Intranet is protected from the Internet by a firewall.

Legitimate Purposes: use by employees, students or other authorised Users for the purpose of supporting the University academic and administrative activities.

Network: the physical and or logical interconnection between devices which includes communication capability that allows one User or system to Connect to another User or system.

Personal Information: means Information about an identifiable individual. The Information does not need to name someone specifically if they are identifiable in other ways. This can include (but is not limited to): name, contact details, date of birth, image, log in details, opinion, employment Information, health Information and financial Information.

Software: the programs used to direct the operation of a computer, including operating systems, patches and applications, and the documentation giving instructions on how to use them.

System Custodian: the individual or group deemed to be the business Custodian of a system.

University: means the Auckland University of Technology (**AUT**) and includes all subsidiaries.

User: all Users of AUT’s ICT systems including, but not limited to, all students, employees, contractors, consultants, other staff, suppliers and visitors.

4. ACTIONS

Information technology is a strategic resource, AUT provides ICT Systems & Services to support the administration, teaching, learning, and research functions of the University.

Strategic Alignment of ICT Systems & Services

AUT is complex both in organisation and technology; requiring that competing ICT needs are carefully evaluated to ensure optimal use of limited resources as well as alignment with institutional strategic goals. ICT Services will partner with business and initiative sponsors to assess the benefits of current and proposed ICT Systems & Services, taking the following aims into account:

- Enabling University strategic goals;
- Leveraging shared, commercial, and existing University systems to maximise return on investment;
- Providing high quality and cost-effective applications which are reliable and have a high Availability;
- Securing key services and ensuring they are well supported;
- Encouraging standardisation and re-use wherever possible.

Management and Support of ICT Systems & Services

Service Desk

ICT Services provides a Service Desk that is available to all Users of AUT ICT Systems & Services. Staff and student specific services, and self-service facilities are available. Service Desk provide service delivery and support to all Users of AUT systems and services.

Requests for ICT Systems & Services

All requests for ICT Systems & Services should be logged with the Service Desk and recorded in the University's service management system. Depending on the nature of the request, it will then be routed to the appropriate process and managed by the relevant service delivery area within ICT Services.

ICT Systems & Services Design and Integration

To facilitate ease of use and ensure maximum benefit from standardisation, applications will be well thought out and integrated into the University's technology architecture. Re-use of applications and integration of Information while maintaining appropriate levels of access is encouraged.

ICT Services provides an architecture and design capability to assist with design, planning and integration of technology solutions. Solutions must be consistent with business continuity and disaster recovery requirements.

Software and integration development undertaken by ICT Services will use common technologies, frameworks, and practices. Designs and code will be appropriately reviewed, and quality assured, and all changes will follow the ICT Services change and release process.

ICT Services managed projects will adopt project management practices appropriate to the size, risk, and business priority of the project.

Third Party Services

To support the diversity of business requirements and processes, the University will utilise both internally and externally hosted solutions, with preference to external hosting particularly for Commodity Services. These services should be chosen on their merits. All outsourcing and procurement of ICT Systems & Services, will be specifically evaluated by ICT Services for supportability, security and sustainability and entered under full legal and commercial due diligence.

Changes to ICT System & Services

ICT Services operates a production release management process to effectively manage changes to AUT's ICT Systems & Services. All changes to ICT Systems and Services will be well managed and adhere to ICT Services' change management process.

Usage of ICT Systems & Services

Acceptable usage

Acceptable use of ICT Systems & Services is defined in the Information and Communications Technology Policy. Unacceptable or prohibited use should be reported to ICT Services for investigation and any required action.

Personal use of the Network

Users may make limited personal use of ICT and Network facilities, provided it does not interfere with use for Legitimate Purposes or conflict with business objectives. All associated electronic communication may be considered the property of the University and are therefore not owned by, or Confidential to, the User.

Your AUT Email address should only be used for AUT related business, the AUT Email address is not intended for personal use.

Users may not use ICT facilities for non-University commercial purposes, for personal gain or for any use that contravenes any University policy without express written permission of the Vice Chancellor or their delegated authority.

ICT Training

From time to time, ICT will make training in general ICT practices, and some widely used systems and platforms, available. Training is highly encouraged for all Users, but, in situations where there are legal or contractual obligations, can be mandatory before access to ICT systems or services is granted.

Identity in ICT Systems & Services

Identity verification

The University reserves the right to verify a User's identity. All Users must have their access to ICT Systems authenticated with a User-ID and a secret password or by some other means that provides equal or greater security.

Passwords must not be disclosed, shared, or revealed to anyone, and must adhere to the Account and Password Standard.

Access to ICT Systems & Services

Access

The principle of least privilege should always be used.

User disconnection

ICT Services has the right to disconnect any User at any time.

Network access

The AUT Network will be logically segmented as per the Security Architecture Standard, and each segment will be protected by firewalls configured according to the Firewall Management Standard. All connections to the Network must meet the Minimum Endpoint Security Standard appropriate to the Network segment or have an exemption from the Chief Technology Officer or their delegated authority. Record of exemptions must be stored in the register of ICT Assets.

Bastion hosts

For high/very high risk systems, administrative access must only be available via secure bastion hosts located in an appropriate Network zone. A secure bastion host is a system which has undergone security screening and is treated as a high risk system. Responsibility for this system lies with the ICT System administrators responsible for the systems and services that it provides access to.

Network Connection

The AUT Network will be logically segmented as per the Security Architecture Standard, and each segment will be protected by firewalls configured according to the Firewall Management Standard. All connections to the Network must meet the Minimum Endpoint Security Standard appropriate to the Network segment or have an exemption from the Chief Technology Officer or their delegated authority. Record of exemptions must be stored in the register of ICT Assets.

Device or Service Disconnection

ICT Services has the right to disconnect from the Network at any time, any device that may impede or reduce the Network’s performance and/or security.

Privacy in ICT Systems & Services

Disclosure

In exceptional circumstances the University reserves the right to examine and disclose activities, the content of messages, and the contents of any electronically stored, processed, or transmitted Information to others when authorised by the Vice Chancellor or their delegated authority. The University may disclose activities to external agencies if legally obliged to do so.

Continuity of Access to ICT Systems & Services

The University reserves the right to grant access to electronic files in order to ensure continuity of day-to-day business operations, for example during a User’s unexpected absence. Access must be authorised by the Vice Chancellor or their delegated authority.

Data Confidentiality

Users should not rely on the Confidentiality of Information or Data transmitted electronically over Networks or stored on a system or service as this cannot be guaranteed without appropriate encryption.

AUT's ICT Systems & Services must comply with the Minimum Application Security Standard. Users utilising other systems and services, e.g. if collaborating with other institutions, should ensure that all Data at rest and in transit encrypted.

Māori Data Sovereignty

Māori data sovereignty concerns the rights and interests of Māori in relation to data that pertains to them, ensuring that data governance aligns with Māori values, aspirations, and philosophies. In the context of AUT and the Te Aronui framework, this means that any data collected about Māori students, faculty, or research that concerns Māori communities and knowledge, must be managed, stored, and analysed in ways that respect Māori cultural values and rights. This translates to meaningful Māori involvement in decision-making processes around data management, safeguarding Māori intellectual property, and ensuring culturally sensitive data practices.

ICT Systems & Services Security Management

Risk assessment

ICT Services will perform Information systems risk assessment, prepare Information systems security action plans, evaluate Information Security products, and perform other activities necessary to ensure a secure Information systems environment.

Vulnerability management

AUT will track vulnerabilities on all AUT assets within the AUT Network to remediate, and minimize, the window of opportunity for attackers. ICT Services will monitor public and private industry sources for new threat and vulnerability Information.

Suspected security incidents

All Users, including contracted third parties will report any observed or suspected ICT security incidents, including loss of ICT assets such as phones, laptops, and external storage devices to ICT Services as quickly as possible.

All security incidents involving the potential or actual compromise of Information Security will be investigated by appropriate personnel and follow the ICT Services Security Incident Response Plan as required.

Inventory and configuration management

All ICT Assets owned or approved by AUT must be recorded in a register held by ICT Services, recording at least the IP address, a unique identifier, the owner and the purpose. Any applicable Network connection exemptions must also be recorded.

ICT Services must be notified of any cloud or Software as a service used to store AUT Data or Information or support any AUT operations or services so it can be recorded and assessed.

ICT Systems & Services are to be managed where possible by a centralised configuration management system or service.

Application software security

All applications must meet the minimum security standards as outlined in the Minimum Application Security Standard unless authorised not to do so by the Chief Technology Officer.

System Custodians are to follow Secure development practices.

System Custodians of any development activities that use private, sensitive or very sensitive Personal Information must ensure that code reviews are incorporated into each phase of the Software development life cycle.

System Custodians of all applications that deal with sensitive or very sensitive Personal Information must perform a security assessment prior to release to production and every two years thereafter.

Endpoint security

All Endpoints should meet the Minimum Endpoint Security Standard unless authorised not to do so by the Chief Technology Officer.

Users must not leave their computers, workstation, or terminal unattended without first invoking a password protected terminal lock, logging-out.

Server security

All applications must meet the Minimum Server Security Standard unless authorised not to do so by the Chief Technology Officer.

ICT Services staff must become familiar with all available security features of each system and service they manage and invoke (harden) these in all cases unless authorised not to do so by the Chief Technology Officer.

Security patches and service packs

The Software of any Network Connected device will be kept up-to-date with the latest security patches and service packs.

- Critical emergency patches as indicated by an internal risk assessment are to be applied as soon as possible.
- High severity security patches are to be applied within 15 days of publication.
- Medium severity to be applied within 30 days of publication.
- Low severity to be applied within 60 days of publication.

Intrusion detection and malware protection

AUT will take all reasonable measures to protect against unauthorised access and the introduction of malicious Software, including viruses. Such measures will be continually reviewed and updated to ensure their ongoing effectiveness.

Monitoring

ICT Services will monitor for security threats across the enterprise’s Network infrastructure and User base.

High and moderate risk systems or services will be added to the AUT central monitoring service with appropriate checks setup to ensure the system or service meets the Minimum Server Security Standard and the Minimum Application Security Standard.

Low risk systems or services can be added as required to the AUT central monitoring service.

Logging

High and Very High risk systems and services must forward appropriate authentication and application logs to the AUT central log service.

All connections to the AUT Network must be logged to a centralised logging service.

Systems and server hosting

AUT systems and services are to be hosted in an ICT Services approved and managed Data centre or external hosting provider.

ICT Services will evaluate service providers who hold private, sensitive or very sensitive Data, or are responsible for an AUT's medium, high or very high risk IT platforms or processes, to ensure these providers are protecting those platforms and Data appropriately.

Information Security

All Users must take all reasonable steps to secure the Integrity, Confidentiality and Availability of Information used for University business.

The University must meet all legislative and contractual obligations relating to the security of Information held within its systems, including but not limited to: Privacy and PCI-DSS compliance.

ICT Systems & Services Availability

Data and Information must be stored on AUT approved secure storage to ensure the Information is available to the organisation should the device be damaged or lost. The What to Store Where Guideline and Research Data Guideline contain guidance of appropriate storage locations.

Data and Information must not be permanently stored on local and removable devices, including memory sticks, laptops, mobile devices and portable disk drives.

All removable devices must have a label and a text file that identifies it as the property of the University.

Business continuity

Heads of business areas are accountable for ensuring that there are alternative means of continuing University business under their direction should ICT Systems & Services be disrupted for an extended period.

Disaster recovery

System Custodians are responsible for ensuring that disaster recovery and business continuity plans are in place and tested for their system or service.

The ICT Services will maintain the ICT Disaster Recovery Plan and will test recovery procedures at least once per year.

ICT Systems & Services Licensing

The University will make every effort to ensure that no Software used on its systems contravenes the Copyright Act 1994.

Users are advised that the University will hold individually liable anyone who breaches copyright using the University's computing systems or other facilities. ICT Services have the right to audit all University systems and remove any Software that breaches the University's obligations under the Copyright Act 1994.

AUT reserves the right to protect its reputation and its investment in computer Software by enforcing strong internal controls to prevent the making or use of unauthorised copies of Software. These controls may include periodic assessments of Software use, announced and unannounced audits of University computers to assure compliance, the removal of any Software found on AUT property for which a valid license or proof of license cannot be determined, and disciplinary actions, in the event of employee violation of this policy.

5. RESPONSIBILITIES

System Custodian

Each University ICT business system will have a formally designated System Custodian at management level who represents a core constituency of system Users. The System Custodian must provide leadership and direction for system development, enhancement, and ongoing operations, including ensuring that appropriate controls for both User access and use of Data are in place. The System Custodian will work closely with the Chief Technology Officer to ensure that the system delivers appropriate levels of service, functionality and reporting to the wider University.

Specific responsibilities include:

- Monitoring internal and external factors to ensure the system is “fit for purpose” including, but not limited to: Legal and contractual obligations; University business drivers and strategic goals; innovation and technology related to the system.
- In conjunction with ICT Services, plans, requests, and manages budgetary requirements for any system development.
- Overseeing, monitoring and where appropriate directing the ongoing enhancement and/or development of the system.
- Overseeing, monitoring and where appropriate directing the day-to-day business usage of the system.
- Ensuring that all Users receive an appropriate level of training in relation to the use of the system.
- Establishing criteria for controlling User access to various functions of the system.
- Ensuring that the storage, use, release, and retention of Data within the system complies with relevant legislation, such as the Public Records Act, Official Information Act, and Privacy Act, University policies, and the AUT Data & Information Governance Framework.
- Ensuring meaningful Māori involvement in the decision-making processes around data management, safeguarding Māori intellectual property, and ensuring culturally sensitive data practices.
- Ensuring that any private, sensitive, or very sensitive AUT Information is appropriately protected.
- Regular review and sign-off of all accounts accessing the system, performed at least annually.

ICT Services:

Are responsible for implementing the Information and Communication Technology Policy, these Procedures, and creating, maintaining and implementing any Guidelines or Standards required to support them.

ICT Services are responsible for ensuring Users and partner organisations are made aware of their obligations.

All Users of AUT ICT Systems and Services

- Must be aware and abide by the Information and Communication Technology Policy and associated Procedures.
- Will not use ICT Systems for any prohibited activity described in the policy or procedures. All Users will at all times act in a responsible, professional, safe manner, maintaining awareness of and compliance with this Procedure and the Information and Communication Technology Policy.
- Must protect the Confidentiality, Integrity and Availability of AUT systems and services Information at all times.
- Will take all reasonable steps to ensure physical protection of University computer facilities.

- Will report breaches in ICT security, loss or theft of ICT assets, and shortfalls in existing security practices or improvements that could be, made to ICT Services.
- Must ensure passwords are not disclosed or used by others.
- Users must not leave their computers, workstation, or terminal unattended without first invoking a password protected terminal lock, logging-out.
- Must use ICT Systems & Services for Legitimate Purposes only.
- Will comply with all controls established by System Custodians.
- Use of ICT Systems and Services must be in compliance with all other AUT policies.
- Will ensure access to AUT high risk Information is provided on a "need to know" basis, based on staff/User role; AUT will not approve unauthorised external or internal access to AUT systems and high risk Information. ICT Services or the System Custodian may be contacted to confirm authorisation of access permitted.
- Will ensure that AUT very sensitive Personal Information should at all times be stored on AUT-approved storage and devices, stored in the least number of locations as possible and, when stored outside of managed high risk approved systems and servers, must be anonymised and appropriately protected. Guidance on AUT-approved storage may be found in the What to Store Where, and Research Data Storage Guidelines.
- Must ensure AUT has purchased fully licensed copies of computer Software, licensed and registered copies of Software programs are placed on computers within the University, and appropriate backup copies are made in accordance with the licensing agreements. No other copies of this Software or its documentation can be made without the express written consent of the Software publisher and AUT.
- Will only install software for Legitimate Purposes.

7. POLICY BASE

Information and Communication Technology Policy

8. ASSOCIATED DOCUMENTS

Employee Discipline Policy

Privacy Policy

Risk Management Policy

Risk Management Procedures

Procurement Policy

Records Management Policy

Records Management Procedures

What to Store Where Guideline

Research Data Storage Guideline

ICT Standards

Account and Password Standard

Minimum Application Security Standard

Minimum Server Security Standard

Change and Release Management Process

ICT Services Security Incident Response Plan

9. FORMS/RECORD KEEPING

All records will be retained as outlined in Responsibilities above and as per the Records Management Policy.

10. DOCUMENT MANAGEMENT AND CONTROL

Procedures Owner:	Chief Technology Officer
Last review:	15 September 2025
Next review:	30 September 2026
Approved by:	Vice-Chancellor
Effective date:	2 February 2024