INFORMATION AND TECHNOLOGY SECURITY POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	September 2023
Next Review	September 2024
Approval	SLT 22/12/168

Purpose:

To ensure Massey University's information and information technology assets are appropriately protected and to ensure information security risks are identified and mitigated.

Key success factors:

- Massey University is protected against unauthorised access to, or unauthorised use or sharing of data which could potentially result in harm to the University or to members of the University community.

- The University is compliant with legal requirements, University policies and any agreements binding the University to implement applicable security safeguards.

- Information security assurance is enabled through clear lines of responsibility and controlled access to university information.

Audience:

This policy applies to all staff, students, third parties (including, but not limited to contractors, consultants, and volunteers) or anyone using Massey University information and communication and technology systems. It applies to all information held for the purposes of the University's operations including the provision of teaching and learning, and research and to those who create, access, process, transmit or store Massey University information.

Policy Statements:

1. The threat landscape and security risks are constantly changing. To reduce risk university staff are expected to complete security awareness and training modules yearly to protect Massey and staff information.

2. All University ICT systems must undergo a security assurance review prior to being purchased to ensure they meet the minimum information security requirements of the University, in accordance with the University's Progressive Procurement Policy and procedures.

3. All University ICT systems must comply with the University's information security and technical standards before being installed into any production environment or handling of any University data.

4. Over the term of its lifecycle, all information must be appropriately classified, and where required, include restrictions on redistribution when transmitted via email or physical mail, storage, and disposal methods in accordance with the Information Security Classification Framework.

5. When changes are proposed to systems, a risk assessment, overseen by the Chief Information Officer, shall be undertaken to identify potential information security risks. Where a risk is identified, the Data Custodian of the system must approve any changes before they are made. All University ICT systems shall have an identified Data Leader, Data Custodian and Data Steward(s) responsible for the risk management of the asset. Information security risks shall be managed in accordance with the University's Risk Management Policy and Framework.

6. Information security and technical standards will be included in design specification prior to procurement for all third party purchased technology or applications. All third-party service providers and agents with access to any University information asset shall comply with all regulatory, legal, and contractual requirements, including University statutes and policy documents.

7. Applying a principle of least privilege, access must be explicitly requested and approved to access non-public facing technology assets. Personal, sensitive, and confidential information will have access controls applied accordingly.

8. Misuse of University information, communication and technology assets will be treated seriously. Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures, and when appropriate, sanctions up to and including dismissal or expulsion may be imposed. Examples of misuse of technology can include, but are not limited to, the unsanctioned installation or running of hacking software, crypto mining software, pirated software, or any other software that may be used to intentionally or negligently compromise the University's information and technology assets.

9. At any time and without prior notice, the University reserves the right to monitor, access, inspect or lawfully disclose any information stored on or transmitted through university information systems (including via a VPN connection) for ensuring compliance with university policy and legal obligations.

Roles and responsibilities:

10. The DVC University Services is the Chief Information Security Officer (CISO) and is accountable for:

    - overseeing the University security programme and ensuring compliance with architecture, policy, standards, regulations, and legislation

    - ensure alignment between information security and business objectives at the strategic level

    - strategic oversight via Crisis Management Team engagement in the event of an emergency (Note: Emergency event includes significant ICT security incident).

11. The Chief Information Officer (CIO) is responsible for:

    - constructing and delivering an information security programme which shall include the creation of an information security strategy, architecture, principles, policy, standards, objectives, and other relevant components

    - coordinating the development of ICT disaster recovery plans and arrangements within the University to ensure that business-critical services are supported appropriately, and that information security is maintained in the event of a disaster

    - developing and maintaining a comprehensive strategic level information security and security risk management programme within the University aimed at protecting Massey's official and classified information

    - monitoring compliance to security policies, architecture, standards and to relevant regulation and legislation

    - approving the isolation or disconnection of any equipment, ICT facility or account from the University network which breaches this policy. The re-enablement of disconnected assets as a result of a breach of this policy will need to be authorised by the CIO and the applicable Head of School or relevant approving authority

- providing oversight of the security assurance review of ICT systems.

12. All technical staff with administrator privileges or those undertaking ICT related work are responsible for:

    - complying with all technical standards when designing, purchasing, configuring, or operating ICT related systems, solutions, or applications.

    - maintaining professional standards of knowledge, skill, and expertise in relevant ICT technical areas.

13. All users are responsible for:

    - complying with information security policies, processes, and standards, and understand their specific responsibilities for information security

    - maintaining the confidentiality and privacy of individuals whose information and records they access

    - immediately reporting any system vulnerabilities, incidents (issues) or technical risks related to information security to the IT Service Desk

    - advise their manager immediately if they identify or suspect that they or any other person may have inappropriate access to private or sensitive information.

Definitions:

Classified Information has been identified and marked to enable protection and effective handling using the New Zealand Government Security Classification System.

Data Leader is a representative of the University's Senior Leadership Team (SLT). Data leaders provide strategic guidance regarding the data requirements of the University.

Data Custodian refers to the business owner of a particular ICT System. This is usually an authoritative head of the respective College, School, Division or Unit within the University who has a level of accountability and/or responsibility around decision making as it applies to a particular technology asset and are responsible for the information that resides and/or is primarily used in their department. This reflects the line management and delegated responsibility applied to a role by the University.

Data Steward is an individual responsible for the day-to-day operational management of an ICT System.

Information Security directly relates to the assurance that the confidentiality, integrity and availability of all information and ICT systems are maintained to the appropriate degree and provides assurance that data is only accessible by those who are authorised to view it, unless a special request is received.

ICT System refers to an information, technology, or communication system used to deliver a business service (such as email), including its computing equipment, business applications, audio visual, data network, telecommunication and other communications systems, storage media and peripheral devices.

Official Information is any information held by an agency subject to the Official Information Act. This includes documents and non-written information.

Security Assurance Review provides confidence that University ICT systems meet security requirements and are resilient against security vulnerabilities and failures. The confidence indicated by the security assurance review represents the level of trust given to a system that shows it is safe to use.

Relevant Legislation and Government Manuals:

Privacy Act 2020
Copyright Act 1994
Official Information Act 1982
New Zealand Information Security Manual
New Zealand Protective Security Requirements

Related Policies and Standards:

Acceptable Use of Technology Policy
Information Security Classification Policy and Framework
Device Security Policy
Information and Records Management Policy
Mobile Device Management Policy
Privacy Policy
Progressive Procurement Policy
Staff Conduct Policy
Technical Standards

Document management control:

Prepared by: Chief Information Officer
Authorised by: DVC, University Services
Approved by: SLT 22/12/16
Date issued: April 2022
Last review: September 2023
Next review: September 2024

Information Security Classification Framework

Purpose: This Framework helps determine what our baseline information security controls are, so that based on its classification, we can mitigate risk

INFORMATION SECURITY CLASSIFICATION			BASIC GUIDELINES ON HANDLING OF THE CLASSIFICATION		
Classification	**Description**	**Information Sharing**	**Transmission**	**Storage** Must comply with Information and Records Management Standard under the Public Records Act 2005)	**Disposal Method** Must comply with Information and Records Management Stand Records Act 2005)
UNCLASSIFIED	**Disclosure of this information to an unauthorised party is not likely to adversely affect the interest/reputation of Massey University or the privacy of any natural persons.** For information which are not publicly available and primarily for internal use. They are information where additional protective markings are not required to increase security, given that the baseline protections for availability and integrity still apply. Most official information does not meet the threshold for a security classification. It is generally referred to as 'unclassified' information and may be marked as such but need not be.	Information that is created and consumed by staff. Intended for internal use, however, may be shared with contractors, students, anyone with a formal, internal relationship with the University (e.g., vendors), or externally as and when needed.	**Electronic Transmission:** • Information can be transmitted without restriction between Massey University staff and students or anyone with a formal relationship with the University. • Ensure correct recipients for transmission to external email addresses. **Paper Transmission:** Sealed envelope stating recipient and postal address e.g., internal mailbox number.	**Electronic Storage:** • Stored in a file or directory accessible to authorised users. **Paper Storage:** Should be stored in a way that are protected against theft, vandalism, or misuse.	**Electronic Disposal:** • Electronic files, magnetic and other storage media should be disposed of in a way that makes compromise unlikely. **Paper Waste Disposal:** UNCLASSIFIED documents are subject to standard secure disposal. They are to be disposed of in a way that makes compromise unlikely, such as depositing the documents in a secure destruction bin at Massey. (Further details – see IRM website).
IN CONFIDENCE	**Disclosure of this information to an unauthorised party would be likely to impede the effective operation of Massey University or adversely affect the privacy of any natural persons.** For all Massey information where the use of information is subject to privacy, legal privilege, obligations of confidence, commercial interests or constitutional conventions, Massey's policy requires staff to take reasonable steps to protect that information from unauthorised disclosure or access. Examples of IN CONFIDENCE information: • Adversely affect the privacy of any person. • Any information that could bring Massey University into disrepute. • Any information that unauthorised disclosure could impede Massey commercial activities, breach constitutional conventions or legal professional privilege. • Any information that unauthorised disclosure would likely result in adverse media attention. • Any information that has been provided in confidence, or where there are contractual requirements for confidentiality.	Information that is created and consumed by authorised staff. Intended for internal use, however, may be shared with contractors, students, anyone with a formal, internal relationship with the University (e.g., vendors), or externally as and when needed – some limitations will apply i.e., a reason for sharing externally and who it is being shared with. **Note:** Personally Identifiable Information (PII) should not be shared externally unless authorised	**Electronic Transmission:** • Information **must be** marked IN CONFIDENCE • IN CONFIDENCE information can be transmitted across external or public networks (including the internet). The level of information contained should be assessed before transmitting. • Username/password access control and/or encryption should be considered. • An appropriate statement should accompany all IN CONFIDENCE information transmitted via email **Paper Transmission** • Documents **must be** posted in a sealed envelope. • May be carried by ordinary postal services or commercial courier firms, provided the envelope/package is sealed. • The envelope must clearly show a return address in case delivery is unsuccessful.	**Electronic Storage:** • Electronic files **must be** protected against inappropriate use or unauthorised access. • Risk mitigation controls must be appropriate and in accordance with the University's Risk Management Framework and the Information Security Manual. **Paper Storage:** IN CONFIDENCE documents should be stored in locked drawers or cabinets with restricted access.	**Electronic Disposal:** • Electronic files, magnetic and other storage media should be disposed of in a way that makes compromise highly unlikely. • Magnetic waste e.g., CDs, tapes, videos **must be** securely disposed of using secure destruction services at Massey. **Paper Waste Disposal** • IN CONFIDENCE documents are to be disposed of in a way that makes compromise highly unlikely i.e., using secure destruction services at Massey. (Further details - see IRM website).
SENSITIVE	**Disclosure of this information to an unauthorised party would be likely to seriously damage the interest/reputation of Massey University or endanger the safety of any natural persons.** Examples of SENSITIVE information: • Endanger the safety of any person. • Seriously damage the interest of Massey if prematurely disclosing information relating to decisions, trade secrets, agreements, or commercials activities. • Impede Massey negotiations (including commercial and industrial negotiations). • Any information that unauthorised disclosure would likely result in prolonged adverse media attention.	Sensitive or restricted information created and consumed by a limited subset of authorised staff. Intended for internal use, however, may be shared with students, contractors, anyone with a formal, internal relationship with the University (e.g., vendors) or externally as and when needed (given it is authorised) – some limitations will apply.	**Electronic Transmission:** • Information **must be** marked as SENSITIVE. • All SENSITIVE information can be transmitted across public networks (this includes the internet) within NZ or across any networks overseas but **must be** encrypted. **Paper Transmission:** • Documents **must be** posted in a sealed and taped envelope and marked SENSITIVE for addressee only. The use of double envelopes may be considered. • May be carried by ordinary postal services or commercial courier firm, provided the envelope/package is properly sealed. • The envelope must clearly show a return address in case delivery is unsuccessful. • The envelope should be addressed to an individual by the name and title.	**Electronic Storage:** • Electronic files **must be** protected against inappropriate use or unauthorised access. • Risk mitigation controls must be appropriate and in accordance with the University's Risk Management Framework and the Information Security Manual. **Paper Storage:** SENSITIVE documents **must be** protected against unauthorised access by storing them separately from other files, and in locked drawers or cabinets. The storage areas should be intruder resistant with security measures applied e.g., building security, door swipe system.	**Electronic Disposal:** • Electronic files, magnetic and other storage media **must be** disposed of in a way that makes reconstruction highly unlikely. • Magnetic waste e.g., CDs, tapes, videos **must be** securely disposed of using secure destruction services at Massey. **Paper Waste Disposal:** SENSITIVE documents are to be disposed of in a way that makes reconstruction highly unlikely, i.e., using secure destruction services at Massey. (Further details - see IRM website).