MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

DATA CLASSIFICATION POLICY

Section	Information Technology Services
Contact	Data Management Specialist
Last Review	NEW
Next Review	September 2022
Approval	SLT 19/10/167
Effective Date	September 2019

Purpose:

To define how data is identified, classified, labelled, and properly handled and protected in accordance with its importance and potential impact to the University. Data must be handled throughout its lifecycle, from creation to disposal. The importance of information varies and therefore requires different levels of protection. Additionally, the policy articulates the government's requirements by applying safeguards so that data, people and assets are protected.

Scope:

This policy applies to all University employees, contactors, volunteers, and any other users authorized to access data stores, information in any medium, and/or information systems. In addition, third parties may be subject to this policy through contractual obligations to the University.

Policy:

- An Information Security Governance Board (ISGB) will be established to oversee the Data Classification (DC) initiative.
- Data Custodians shall identify and authorise the security classification of their information systems in accordance with the Data Classification Framework (DCF)
- Data Stewards shall manage access to those systems and stores in compliance with the DCF
- Departments will ensure that all data is appropriately identified, including restrictions on redistributions when transmitted via email or physical mail, according to the DCF
- Data Custodians will review the department's progress annually. Metrics will be presented to the steering committee, including the total number of data stores and systems identified and their associated classification status
- Data Custodians will work with the IT security department to ensure appropriate asset protection measures are in place relative to the data's classification.

Definitions and Roles:

Data Classification in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The classification of data determines what baseline security controls are appropriate for safeguarding that data. Massey University has three sensitivity levels, or classifications: Public; In-Confidence; Sensitive (Appendix 1).

Information Security Governance Board provides guidance and final determination on the classification of data consistent with the Data Classification Framework

Data Custodians have direct responsibility for the data that resides and/or is primarily used in their department. The Data Custodian is accountable for authorising and reviewing the classification of data.

Data Stewards are individuals responsible for the day to day management of the data, including operational requirements of data quality, compliance with requirements, conformance to policies and standards, security controls, and identifying and resolving data issues.

Data Users are individuals who create new data at any point during its lifecycle. Anyone within the organisation can be a data user.

Relevant legislation:

- Contract and Commercial Law Act 2017
- Copyright Act 1994
- General Data Protection Regulation 2018
- Official Information Act 1982
- Privacy Act 1993
- Public Finance Act 1989
- Public Records Act 2005.

Legal compliance:

- *Contract and Commercial Law Act 2017*
  Includes provisions concerning the legal effect of information that is in electronic form or that is communicated by electronic means (s 211), default rules about the time and place of dispatch and receipt of electronic communications (s 212 – 217), key provisions concerning the use of electronic technology to meet certain legal requirements (s 218 – 221), provisions that specify certain legal requirements that may be met by using electronic technology (s 222 –236).
- *Copyright Act 1994*
  Contains references to the requirements for documenting copyright in original works, transferring copyright and licensing for use/copying. Includes documentation requirements for hearings of the Copyright Tribunal. Copyright Regulations also apply.
- *General Data Protection Regulation 2018*
  Establishes a data protection framework to ensure enhanced data protection and privacy rights for European Union (EU) residents. It imposes a comprehensive set of principles and obligations with which a lot of organisations operating or offering products and services for EU residents must comply, including all NZ universities.
- *Official Information Act 1982*
  Provides for access to official information, except where specific reasons for withholding it exist, such as national security or the protection of personal privacy.
- *Privacy Act 1993*
  Establishes a set of privacy principles to ensure the protection of personal privacy in respect of both public and private sector organisations. The Act is of prime importance and should be clearly understood by all information management professionals.

- *Public Finance Act 1989*
  Covers the reporting requirements of the Crown, Government Departments and Crown Entities, including requirements for Audit Office issuing of Audit Opinions.
- *Public Records Act 2005*
  Provides for the selection of public records and archives for creation, maintenance and retention. Directs that public records and archives may only be destroyed or disposed of with the authority of the Chief Archivist. Provides for the deposit of public archives with the Archives of New Zealand and describes conditions for the management of material so deposited. Sets out the powers of the Chief Archivist in respect of current public records.

Related procedures / documents:

- Data Classification Framework
- Data Management Policy
- Information and Records Management Policy
- Internet Use and Digital Communications Policy
- Official Information Policy

Document Management Control:

Prepared by: Data Management Specialist, on behalf of Chief Information Officer
Authorised by: DVC, Finance and Technology
Approved by: Senior Leadership Team
Date issued: September 2019
Next review: September 2022
Effective Date: September 2019

Data Classification Framework: The classification of data based on its sensitivity

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

SECURITY CLASSIFICATION			BASIC GUIDELINES ON HANDLING OF THE CLASSIFICATION		
Classification	**Description**	**Data 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.	Data 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:** • Data 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.	Data 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 data 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 data 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 data 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 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).