Information Classification Standard

Purpose

The purpose of this policy is to describe how information within Unitec should be classified in a manner that is appropriate for its level of sensitivity, to protect it from being intentionally or accidentally being compromised. The sensitivity of information held by Unitec varies significantly from information that can be shared openly with the public through to information that if compromised could cause significant harm to individuals (staff or students) or to the reputation of the institute.

Classified information is material that an organisation deems to be sensitive and must be protected with added security controls. Information is considered classified when sensitivity and privacy meta-data is attached to it via an information system.

Classification meta-data makes it possible for information access to be restricted, as required by legislation or regulation, to groups of people with the need to know. Specifically, the meta-data is used to prevent the mishandling of the information, which might very well incur penalties – should the breach be significant.

Unitec has based the classifications in this document from the Information Classification Standards that the New Zealand government uses to enable and support appropriate sharing of government information.

Scope

This standard applies to all information that Unitec creates, receives, or stores while conducting its business.

It applies to content collected, created, or managed anywhere within the Unitec information systems – whether it is generated by staff, contractors, or students.

Policy Statement

This section details the relevant information classifications from PSR, that we apply as meta-data to our information assets and systems.

The Government's Information Classifications framework provides a framework for assessing the potential harm should government information be compromised and defines the minimum requirements for protecting government information – see https://www.protectivesecurity.govt.nz/classification-system.

Classifying our information according to its sensitivity enables us to apply additional security and access controls to protect it, as necessary.

Information classifications are mandatory.

Which Information Classifications?

Unitec will use the following Government Policy & Privacy Classifications for its information:

- **UNCLASSIFIED**
- **IN-CONFIDENCE**
- **SENSITIVE**
- **RESTRICTED***

***Restricted** is a higher information classification that is technically a National Security classification, but we would be using it in a different context. Its use is reserved for the most secure information internally.

Classifications Table

The following table contains definitions, examples and the expected treatment for information assets that meet the requisite definition. Please refer to Information Classification Controls to review the security controls that realise the correct level of information protection.

- If in doubt about which classification is the correct one, please refer to Digital for guidance.
- If multiple classifications might apply, the highest classification must be applied.

Information Classification	Description	Examples	Treatment
UNCLASSIFIED	Information that doesn't fall within any of the below categories.	• Information published on our website • Meeting agendas or minutes that are required to be notified under LGOIMA • Finalised policies and procedures	Can be freely shared internally or externally.
IN-CONFIDENCE	The document contains confidential and/or commercially sensitive information.	• Programme documentation • Contracts and supplier documentation such as invoices • Internal meeting minutes • Project reports • Draft policies and procedures	Before disclosure, information should be reviewed for potential withholding grounds under the OIA.
SENSITIVE	The document contains sensitive information relating	• Identity documentation	Information can only be disclosed if an exception applies

	to identifiable individuals.	• Personal contact details • Financial information • Enrolment records • Employment details	under the Privacy Act or other legislation.
RESTRICTED*	Access to this information must be restricted to a limited group (e.g., ELT/Council/Minister)	• Strategic working papers • Change proposals	All information needs to be treated on a need-to-know basis. For internal use only.

Associated Procedures

The following documents are to be read in association with this Policy:

- Information Classification Controls
- Creation & Maintenance of Electronic Records Procedure

Responsibilities

Information Owners are responsible for ensuring it is properly classified, and access is effectively managed. Information Owners are also responsible for communicating this to other individuals who in their duties might handle, store, or process the information.

All Unitec kaimahi who access, use, and share information are responsible for understanding and following the rules relevant to the information's classification.

Digital is responsible for providing advice, appropriate system security measures and active monitoring including the architecture of these systems and services.

Definitions

Term	Definition
Information	refers to documents, data, emails, paper documents, phone recordings, video uploads, analytic reports, regardless of format, location, application
Information System	refers to a solution or application that is used to manage or access information for example digital data stores and physical filing cabinets

Information Owners	Senior managers who are accountable for the activity that the information relates to.
Unitec kaimahi	includes all full and part-time permanent, temporary, adjuncts, and contractors
Unitec ākonga	Includes all people who are or have been learners/ enrolled as a student at Unitec

Reference Documents

Other related Unitec Policies

- Unitec's Privacy Policy
- Unitec's Electronic Devices and Systems Policy
- Unitec's Intellectual Property Policy
- Records Management Policy

Related Legislation

- Public Records Act 2005
- Privacy Act 2003
- Official Information Act 1982
- Local Government Official Information and Meetings Act 1987

Approval Details

Version number (this version)	2.0	**Issue Date (this version)**	10/06/2025
Version History (Amendments made to this version)	Date of amendment/s: • 16/06/2025	Amendment/s: • Updated format to Unitec Standard Policy Template. Updated Classification labels to remove sub-categories. Updated descriptions and definitions of 4 remaining label categories.	
Consultation Scope (if appropriate)	Key stakeholders consulted in the review of this policy: • Regional Digital Operations Lead Rohe 1 • Director Legal • IT Infrastructure and End User Support Manager		
Approval authority	SLT	**Date of Approval**	30/05/2025
Policy Sponsor (Has authority to approve minor amendments)	• Regional Digital Operations Lead Rohe 1	**Policy Owner**	Records and Information Management Specialist
Contact Person	James Meyer	**Date of Next Review**	10/06/2026