Information Classification Controls

Purpose

This document describes the controls in place for the Information Classes listed in Unitec 's **Information Classification Standard**.

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.

Procedure

This section contains the security controls that should be applied to information, for each of the Information Classifications listed. Controls are divided in the following areas: Storage; Use, Copy, or Share; Removal or Transport; Archive or Delete.

While information should always be classified correctly, there is a chance it may not be, and it is therefore better to be more secure and apply these controls when possible.

UNCLASSIFIED

The controls in the **UNCLASSIFIED** section are considered more a *should* than a *must*. Information with this information classification is the routine information collected or created during business operations. It may be shared freely with people internal to the organisation but should be reviewed by the information owner prior to being shared.

Storage

1. Physical materials and equipment with an **UNCLASSIFIED** marking should be stored in a Security Zone 1 (Public access area) or higher.
2. Electronic information with an **UNCLASSIFIED** marking should be protected against unauthorised internal use or external intrusion through two or more mechanisms:
    a. User challenge and authentication (requiring username/password, digital ID, or digital certificate)
    b. Logging use at level of individual

    c. Firewall and intrusion detection systems and procedures.
    d. Server authentication
    e. Security measures specific to the operating system or application you use.
3. Electronic information with an **UNCLASSIFIED** marking should only be stored in locations authorised by the Unitec. This may be on the Unitec Public Website.

Use, copy or sharing.

1. When communicating **UNCLASSIFIED** information via email externally it must hold the unclassified label.

Removal or transport

1. Removal of **UNCLASSIFIED** information is expected when outside the controls of Unitec, since data is treated are released publicly.
2. information may be carried by post, courier service, or your mail delivery staff.
3. The envelope must clearly show a return address if undeliverable. To protect Unitec ’s privacy, you can use a return PO Box.
4. Never mark classifications or protective markings on envelopes.

Archive or disposal.

1. Archival and disposal of public records must comply with the Public Records Act 2005.
2. Refer to Unitec ’s information and Records Management Policy & Disposal of Records Procedure.
3. Archive or dispose of **UNCLASSIFIED** information or equipment by the arrangements and procedures.
4. When you dispose of electronic Unitec information, ensure the waste can’t be reconstructed or used.

IN-CONFIDENCE

The controls in the **IN-CONFIDENCE** section are intended to restrict access as much as is *reasonably practical*, because information with this information classification is either commercially sensitivity, or confidential. Please refer Information Classification Standard for more details.

Access Management

1. A **IN-CONFIDENCE** information classification may limit access to and apply special handling requirements to the information.

Storage

1. Physical materials and equipment with an **IN-CONFIDENCE** marking should be stored it a Security Zone 2 (work areas) or higher. However, if appropriately secured and access controlled, **IN-CONFIDENCE** information and equipment can also be stored in Security Zone 1 (public access area)
2. Electronic information with an **IN-CONFIDENCE** marking should be protected against unauthorised internal use or external intrusion through two or more mechanisms:
    a. User challenge and authentication (requiring username/password, digital ID, or digital certificate)
    b. Logging use at level of individual
    c. Firewall and intrusion detection systems and procedures.
    d. Server authentication
    e. Security measures specific to the operating system or application you use.

3. Electronic information with an **IN-CONFIDENCE** marking should only be stored in locations authorised by the Unitec.

Use, copy or sharing.

1. Protect **IN-CONFIDENCE** information against accidental or opportunistic compromise during use, such as clearing away documents from desks after use.
2. You must have permission from the Information Owner prior to printing or copying **IN-CONFIDENCE** information.
3. Before disclosure, **IN-CONFIDENCE** information should be reviewed for potential withholding grounds under the OIA.
4. Only reproduce **IN-CONFIDENCE** information when necessary and keep the number of copies to a minimum. All reproduced information must retain the original marking or higher.
5. Consider the sensitivity of the information and if appropriate, use encryption when emailing or transmitting **IN-CONFIDENCE** information. Ensure your address list is correct.

Removal or transport

1. Removal of **IN-CONFIDENCE** information or equipment from your premises should be authorised by the Information Owner or controlling organisation and in accordance with Unitec ’s policy.
2. **IN-CONFIDENCE** information must only be shared using email or direct linking from OneDrive. The platform will protect the information automatically when this classification is in use.
3. When being sent by post the envelope must clearly show a return address if undeliverable. To protect the Unitec ’s privacy, you can use a return PO Box.
4. Never mark classifications or protective markings on envelopes.

Archive or disposal.

1. Archival and disposal of public records must be done in accordance with the Public Records Act 2005.
2. Refer to Unitec ’s information and Records Management Policy & Disposal of Records Procedure
3. Archive or dispose of physical **IN-CONFIDENCE** information or equipment by the organisation’s arrangements and procedures.
4. When you dispose of electronic Unitec information, ensure the digital waste cannot be reconstructed or used. For example, appropriate disk scrubbing processes must be used during hardware asset disposal.

SENSITIVE

The controls in the **SENSITIVE** section are intended to manage access as *a need-to-know basis*, because this information is commercially sensitive or is highly sensitive personal information about kaimahi or learners/ākonga. Please refer Information Classification Standard for more details.

Access Management

1. A **SENSITIVE** information class may further limit access and apply special handling requirements to the information in accordance with Unitec ’s policies and procedures. Refer to your security team to understand access requirements.

Storage

1. Keep Unitec information at **SENSITIVE** information or equipment physically stored in Zone 2 in a lockable storage area or cabinet when not in use. When in use, material or equipment should not be left unattended or unsecured.
2. In a storage facility, **SENSITIVE** information and equipment should be protected through controlled access to the storage areas, and through a secure physical environment.
3. Electronic information (including databases) at **SENSITIVE** should be protected against unauthorised internal use or external intrusion through two or more mechanisms:
    a. User challenge and authentication (requiring username/password, digital ID, or digital certificate)
    b. Logging use at level of individual
    c. Firewall and intrusion detection systems and procedures.
    d. Server authentication
    e. Security measures specific to the operating system or application you use.
4. Electronic information with a **SENSITIVE** marking should only be stored in locations authorised by Unitec.

Use, copy or sharing.

1. Protect **SENSITIVE** information against accidental or opportunistic compromise during use, such as clearing away documents from desks after use.
2. Information at **SENSITIVE**, must be used in Zone 2 (Work Areas).
3. Apply Encryption for emailing or transmitting **SENSITIVE** information across public networks within New Zealand or across any networks overseas using a system approved by Digital.
4. You must obtain Information Owner agreement prior to printing, copying, or sharing **SENSITIVE** information. Printing, copying, reproducing, or sharing may be prohibited by the Information Owner.
5. Copies should not be left unattended on printers or devices.
6. All reproduced information must retain the original markings or higher. Override and justification will be required to lower the classification level.
7. Face-to-face or virtual conversations and meetings discussing or sharing **SENSITIVE** information must be held only in secured areas (Zone 2) and using only accredited Digital systems and networks the same classification level to prevent information compromise.
8. When communicating **SENSITIVE** information via email externally, include a communication of the recipient's legal and destruction obligations if the incorrect party receives it.
9. **SENSITIVE** information should not be accessed on a non-Unitec device or accessed on a public network.
10. Restrictions are put in place for information marked with the **SENSITIVE** classification from being sent or shared with parties outside Unitec. These include restrictions to email/ copy to an external storage device / and Printing without an override and justification provided.

Removal or transport

1. Removal of **SENSITIVE** information or equipment from your premises should be authorised by the Information Owner in accordance with Unitec 's policy and basis of real need. For example, when going to a meeting.
2. You must use security measures to protect marked information when it is in transit.
3. **SENSITIVE** information or equipment may be carried by safe hand, postal service, or commercial courier service for domestic transport.
4. Never mark classifications or protective markings on external envelopes.

Archive or disposal.

1. Archive and disposal of public records must be done in accordance with the Public Records Act 2005.
2. Waste of **SENSITIVE** information refer to Unitec ’s information and Records Management Policy & Disposal of Records Procedure.
3. Must not be disposed by standard rubbish or recycling collection.
4. Information Owner may require shared information to be returned for archival or disposal.
5. Only appropriate NZSIS-approved equipment systems must be used for destruction of paper waste.
6. ICT media and equipment must undergo sanitisation or destruction in accordance with the NZISM 13. Media and IT Equipment Management, Decommissioning and Disposal.
7. When you dispose of electronic Unitec information, ensure the waste cannot be reconstructed or used.

RESTRICTED

RESTRICTED information has similar controls to **SENSITIVE**, but **RESTRICTED** will have stricter access management. **RESTRICTED** is a National Security classification, to be used when compromise of the information is likely to adversely affect the national interest of Unitec.

Access Management

1. A **RESTRICTED** information classification is enforced to limit access and apply special handling requirements to the information in accordance with Unitec ’s policies and procedures. Refer to your security team to understand access requirements.

Storage

1. Keep Unitec information at **RESTRICTED** information or equipment physically stored in Zone 2 in a lockable storage area or cabinet when not in use. When in use, material or equipment should not be left unattended or unsecured.
2. In a storage facility, **RESTRICTED** information and equipment should be protected through controlled access to the storage areas, and through a secure physical environment.
3. Electronic information (including databases) at **RESTRICTED** should be protected against unauthorised internal use or external intrusion through two or more mechanisms:
    a. User challenge and authentication (requiring username/password, digital ID, or digital certificate)
    b. Logging use at level of individual
    c. Firewall and intrusion detection systems and procedures.
    d. Server authentication
    e. Security measures specific to the operating system or application you use.
4. Electronic information with a **RESTRICTED** marking should only be stored in locations authorised by Unitec.

Use, copy or sharing.

1. Protect **RESTRICTED** information against accidental or opportunistic compromise during use, such as clearing away documents from desks after use.
2. Information at **RESTRICTED**, must be used in Zone 2 (Work Areas).
3. Apply Encryption for emailing or transmitting **RESTRICTED** information across public networks within New Zealand or across any networks overseas using a system approved by Digital.

4. You must obtain Information Owner agreement prior to printing, copying, or sharing **RESTRICTED** information. Printing, copying, reproducing, or sharing may be prohibited by the Information Owner.
5. Copies should not be left unattended on printers or devices.
6. All reproduced information must retain the original markings or higher. Override and justification will be required to lower the classification level.
7. Face-to-face or virtual conversations and meetings discussing or sharing **RESTRICTED** information must be held only in secured areas (Zone 2) and using only accredited Digital systems and networks the same classification level to prevent information compromise.
8. When communicating **RESTRICTED** information via email externally, include a communication of the recipient's legal and destruction obligations if the incorrect party receives it.
9. **RESTRICTED** information should not be accessed on a non-Unitec device or accessed on a public network.
10. Restrictions are put in place for information marked with the **RESTRICTED** classification from being sent or shared with parties outside Unitec. These include restrictions to email/ copy to an external storage device / and Printing without an override and justification provided.

Removal or transport

1. Removal of **RESTRICTED** information or equipment from your premises should be authorised by the Information Owner in accordance with Unitec 's policy and basis of real need. For example, when going to a meeting.
2. You must use security measures to protect marked information when it is in transit.
3. **RESTRICTED** information or equipment may be carried by safe hand, postal service, or commercial courier service for domestic transport.
4. Never mark classifications or protective markings on external envelopes.

Archive or disposal.

1. Archive and disposal of public records must be done in accordance with the Public Records Act 2005.
2. Waste of **RESTRICTED** information refer to Unitec 's information and Records Management Policy & Disposal of Records Procedure .
3. Must not be disposed by standard rubbish or recycling collection.
4. Information Owner may require shared information to be returned for archival or disposal.
5. Only appropriate NZSIS-approved equipment systems must be used for destruction of paper waste.
6. ICT media and equipment must undergo sanitisation or destruction in accordance with the NZISM 13. Media and IT Equipment Management, Decommissioning and Disposal.

When you dispose of electronic Unitec information, ensure the waste cannot be reconstructed or used.

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.

Reference Documents

This document should be read in conjunction with:

Other related Unitec Policies

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

Related Legislation

- Public Records Act 2005
- Privacy Act 2020
- Official Information Act 1982
- Local Government Official Information and Meetings Act 1987

Appendix I – Security Zones

Security Zones are areas with defined security controls based on who may have access to the area. These zones will often have different types of physical security separating them to limit movement between the zones. For additional information, refer to Security zones | Protective Security Requirements

Zone 1: Public Access Areas

These are unsecured areas including out-of-office working arrangements. They provide limited access controls to information and physical assets where any loss would result in a low to medium business impact. They also provide limited protection for people.
Examples of public access areas are:

- building perimeters and public foyers
- interview and front-desk areas.
- temporary out-of-office work areas where the agency has no control over access.
- field work, including most vehicle-based work.
- public access parts within multi-building facilities (for example cafes or shops).

Permitted uses.
In zone 1, you can:

- store information and physical assets needed to do business classified as UN-CLASSIFIED or INCONFIDENCE
- Use SENSITIVE information.

Zone 2: Work Areas

These are low-security areas with some controls. They provide access controls to information and physical assets where any loss would result in a business impact up to very high. They also provide some protection for people.
Zone 2 areas allow unrestricted access for your people and contractors. Public or visitor access is restricted.
Examples of work areas are:

- normal office environments
- normal out-of-office or home-based worksites where you can control access to areas used for your business.
- interview and front-desk areas where your people are separated from clients and the public.
- vehicle-based work where the vehicle is fitted with a security container, alarm, and immobiliser.

Permitted uses.

In zone 2, you can:

- store information and physical assets needed to do business classified as UN-CLASSIFIED or INCONFIDENCE, SENSITIVE or RESTRICTED

Approval Details

Version number	1.0	**Issue Date**	10/06/2025
Version History	Date of amendment/s: • Insert Amendment Date	Amendment/s: • Insert reason for amendment	
Approval authority:	SLT	**Date of Approval**	30/05/2025
Procedure Sponsor **(Has authority to approve minor amendments)**	• Regional Digitial Operations Lead Rohe 1	**Procedure Owner:**	Records and Information Management Specialist
Contact Person	James Meyer	**Date of Next Review**	10/06/2026