TRANSPOWER

Keeping the energy flowing

Information Security Classification and Handling Policy

1. Policy overview

The purpose of the Information Security Classification and Handling Policy is to ensure that Transpower's information is stored, transmitted and disposed of securely to manage business and legal risk.

The Policy provides requirements for applying security/access classification tags and applying the appropriate labelling and handling procedures to protect the security, confidentiality, integrity, and availability of information for its access, storage, transfer and disposal.

2. Summary table

This Policy provides minimum requirements for classifying and handling unstructured[1] information created, received, stored or maintained by Transpower. It sets out the requirements and expectations that ensure that appropriate controls are applied to all business information.

This Policy includes protocols and practices for the storage, transmission and disposal of information in the Information Handling table as Appendix 2. The 'Information Handling' table is a living document which will evolve in response to changes in the business environment.

This Policy supports information classification and handling independent of the technology platform used to enable user access, information control and transmission within Transpower, or externally to third parties.

This Policy does not set requirements for cyber or system/application security classification, but supports these requirements through applying security and access classification at the document or item level.

Classifying information assists in the selection and application of appropriate controls to protect the confidentiality, integrity and availability of Transpower's information. It also assists Transpower staff in the appropriate handling of information including its storage, transfer and disposal.

To be effective this Policy must be easy to apply and not impede normal business practice. Ideally this Policy will be applied through default application configurations, automation and supporting tools, e.g. standardised document and email templates and inherited metadata from storage and management applications.

[1] See Appendix 1: Glossary for definitions

3. Roles and responsibilities

The Chief Executive is accountable under the Public Records Act 2005, for ensuring that Transpower complies with legislative requirements for recordkeeping and information management practice.

Managers must:

- Observe the minimum requirements of the Information Security and Handling Classification Policy (and any authorised supporting Guidelines and Standards) throughout its lifecycle.
- Support their staff to comply with this Policy by providing time or resources to undertake information management activities, information governance roles and any relevant training required to ensure staff understand and comply with this Policy.

Information Management team must:

- Develop, implement and maintain Security and Handling Classification Guidelines and Procedures, in association with business partners and stakeholders, as necessary.
- Work with business managers to define their security and handling classification requirements and identify the appropriate classification levels for the management of information.

Transpower Personnel (including contactors and sub-contractors) must:

- Manage their information in compliance with the Information Security and Handling Classification Policy.

4. Scope

This is an organisation-wide Policy. It applies to all information created, received, transmitted, managed or stored by Transpower in the conduct of its affairs, independent of media or format, by all staff and/or third parties.

Information may be contained or transmitted in a variety of media, for example: printed documents, hand written notes, photographic images, videos, electronic documents, emails, web pages, digitised voice mail and audio records.

This Policy applies to anyone delivering work on Transpower’s behalf, defined for the purpose of this Policy as “Transpower Personnel”.

In practice this includes all Transpower staff (permanent, fixed term or casual) and all work done by any third party on behalf of Transpower (including service providers, contractors and/or consultants).

5. Information in scope

This Policy applies principally to unstructured information.

The Policy applies to all unstructured information regardless of format i.e. electronic or physical. It must be applied when information is created, stored, transferred, or disposed of within Transpower, or externally where Transpower shares information with another entity. It is the responsibility of all Transpower personnel and any authorised third parties to handle information according to its classification.

Note: This Policy does not cover 'personal' information which an employee creates or retains for non-work purposes within Transpower systems (see the Security Awareness & Appropriate Usage Policy).

6. Privacy and confidentiality obligations

All employees and contractors must maintain the privacy and confidentiality of Transpower information. This requires all staff to identify the types of information held, and to treat it appropriately.

This includes considerations such as privacy of personal information, commercial confidentiality requirements, intellectual property, legal privilege, Official Information Act requests and national security obligations.

7. Policy Statements

Transpower's Information Security and Handling Classification Policy is described through the following policy statements (7.1 & 7.2).

7.1 Information is classified

Information must be classified appropriately as inappropriate classification (over/under classification) may result in:

- Unintentional, or intentional, damage to Transpower, its reputation, and/or its ability to carry out its functional responsibilities or services
- Unnecessary restriction of access, resulting in reduced productivity, duplication and rework and higher costs.

7.2 Information is classified according to a defined level

All information has an information security classification, according to pre-defined business rules.

- This classification applies regardless of the medium on which the information is stored or displayed (physical or electronic).
- The security classification determines the security and physical controls needed to protect the integrity, availability and confidentiality of the information, while ensuring information is accessible to authorised users for legitimate business purposes.
- The Transpower defined classification levels are:
  - **PUBLIC**
  - **IN CONFIDENCE**
  - **SENSITIVE**
  - **RESTRICTED**

7.2.1 PUBLIC

Information that is intended to be available in the public arena.

Usage Notes:

There are no protection requirements for this category of information beyond ensuring the integrity of the information at the point of dissemination, e.g. Information must be published in a non-editable format such as PDF and website-based information must be protected against unauthorised modification.

Examples:

- External web site content
- Published corporate forms
- Brochures
- Reports
- Current and annual transmission pricing information.

7.2.2 IN CONFIDENCE

Information that relates to Transpower's day-to-day business activities and may include information which relates to its corporate functions, commercial activities and other information which if inappropriately released could impact Transpower's image, revenue or services.

Usage Notes:

This is the default classification for any information used as part of Transpower's normal course of business that is not published in the PUBLIC domain or classified as SENSITIVE or RESTRICTED.

Information in the IN CONFIDENCE classification can be stored in any Transpower managed system with controls sufficient to meet business requirements for integrity, availability and confidentiality.

Examples:

- Internal forms and templates
- Corporate Policies, Procedures and Guidelines
- Position Descriptions
- The bulk of internal business documents.

7.2.3 SENSITIVE

Information, which if compromised could expose Transpower to breaches of personal privacy legislation or breaches of commercial confidentiality. This includes personally identifying information about individuals, either private citizens or Transpower employees; information about agreements with Transpower's commercial partners or contracted third parties.

Usage Notes:

Information that should be protected from accidental release for legal, ethical or commercial reasons is classified as SENSITIVE.

Information relating to Transpower's administration of its legislative functions is classified as SENSITIVE.

SENSITIVE information is not limited to Transpower-specific information. This information may include documents sourced from an entity, about an entity, an individual or about Transpower that are legally privileged.

Examples:

- General commercial contracts and agreements
- Information relating to employee or legal disputes or investigations
- Information relating to an organisational change that affects employees
- Treasury Policy and investment information
- Legal advice
- Pricing information with customers associated with new projects

7.2.4 RESTRICTED

Information, which if compromised or released could prejudice Transpower's negotiations with government or third parties or seriously damage Transpower's image, services or revenue.

This classification also includes information which if compromised or released could adversely affect the economic well-being of New Zealand.

Examples:

- Major commercial contracts and agreements
- Board Papers and correspondence
- Correspondence with regulators on Market Systems policies
- Certain types of correspondence with Ministers
- Schematics of significant, security-sensitive portions of the Grid network

7.2.5 Special handling

Transpower may manage a small amount of information which could be classified above the Transpower information security classification levels and requires special handling. Where this applies the NZ Information Security Manual (NZISM) classifications **Secret** and **Top Secret** will apply for consistency across government entities, and exchange of information with any relevant agencies.

Security Classifications – National Security	Electronic Storage	Access and Transmission	Disposal
TOP SECRET: Compromise would damage national interests in an exceptionally grave manner. Access: Authorised personnel	Not connected to internet or Transpower corporate realm.	Not connected to internet or Transpower corporate realm.	Should be disposed of in a way that makes reconstruction highly unlikely, using an approved secure delete facility, degaussing or physically destroyed.
SECRET: Compromise would damage national interests in a serious manner. Access: Authorised personnel	Not connected to public internet or Transpower corporate realm.	Not connected to public internet or Transpower corporate realm.	Should be disposed of in a way that makes reconstruction highly unlikely, using an approved secure delete facility, degaussing or physically destroyed.

7.2.6 Classification is not static

Information classification is not fixed and static. Information classification may change relevant to its circumstances, e.g. when moving from storage, to transmission or disposal actions, or due to time bound restrictions like legal holds or embargoes, e.g. financial performance information moving from SENSITIVE (before it is released) to PUBLIC once it is released.

Usage Notes:

Information must not be declassified without the approval of the relevant information owner or the appropriate governance authority.

For advice on declassification, please contact the Information Management team.

7.2.7 Classification is supported automated and enabled

Information classification must not be onerous to apply. It must be supported by mechanisms that enable users to apply the classification with the minimum of effort, such as default labelling, pre-populated templates for documents , embedded labels in printed documents and ‘boiler-plate’ statements for contracts.

Advice and guidance will be available to business units and functions, e.g. specifically tailored ‘cheat-sheets’ for use in different areas of the business. Automation will be used where practicable, including toolbars in Office applications and inherited metadata in document management systems.

8. Information is handled appropriately

Information must be handled (stored, accessed, transferred, or disposed of) in accordance with its classification. Once the information has been correctly classified, the **Information Handling Table** that is attached to this Policy can be used to determine the actions and controls that are required for the storage, access, processing, transmission, and disposal of that information.

Usage Notes:

The **Information Handling Table** (attached to this Policy as an Appendix) is intended to be maintained independently as a ‘living document’. The table will be updated as Transpower policies and approaches evolve. It will be published as a linked document rather than a static part of this Policy document.

This Policy does not specify the precise mechanisms to implement the handling requirements, the intent is for them to be practically implementable. For IT systems the handling requirements should, where possible, be built into the system specifications and articulated in any design requirements or documentation.

9. Information is properly labelled

Information and documents (whether electronic or printed) are to be marked or labelled with the appropriate classification. It is the responsibility of the individual who creates or transmits the information or document to classify and label it correctly. However, if a staff member is required to handle an item that has not been marked or labelled appropriately, then they must ensure that it is so marked or labelled before it is further dealt with.

Where doubt exists about an item classification the individual should contact the Information Management team for guidance. Where a document is perceived to be highly sensitive, the matter should be logged as a security incident with the Transpower Service Desk.

The following are examples of approaches to follow in order to mark or label particular types of information:

- Documents and correspondence are to be labelled with the appropriate classification on every page, where practical to do so. This can be by way of headers, footers or watermarks.
- Emails should be marked in the subject line or body of message, where they are SENSITIVE or RESTRICTED.
- If an item is not marked or labelled with a classification, the information must be treated as IN CONFIDENCE as a minimum.

10. Legal exemptions

Transpower's information is subject to Official Information Act and Privacy Act requests. Each request must be responded to in compliance with the relevant legislation, not in accordance with the handling requirements outlined in this document. For example, it is possible that a document labelled IN CONFIDENCE or SENSITIVE is required to be released in response to a request under the relevant legislation.

Requests of this type should be referred to Transpower's Legal team.

11. Monitoring and compliance

Compliance to this Policy will be monitored using compliance mechanisms such as technology based products, *ad hoc* internal assurance audits or via formal independent audits.

Contact

For more information, contact the Enterprise Information Manager.

Related legislation

This Policy has been developed in consideration of the Public Records Act 2005 and may also may be referred to in meeting the requirements of the Official Information Act 1992.

Related external standards

This Policy aligns to the:

- Archives New Zealand mandatory Records Management Standard for the Public Sector

It is also supported by the:

- Information and documentation -- Records management -- Part 1: Concepts and principles (ISO 15489-1:2016)
- ISO 55001:2014 Asset management -- Management systems -- Requirements

Related internal policies

This Policy should be read in conjunction with the following policies:

- Information Management Policy
- Retention and Disposal Schedule – Corporate
- Retention and Disposal Schedule - Operations
- Security Awareness & Appropriate Usage Policy
- Information Security Policy
- Privacy Policy
- Risk Management Policy

Policy approval

Policy approved by Transpower's Board of Directors, People and Performance Committee or Chief Executive (as applicable).

Policy Owner	**Chief Executive**
Effective Date	August 2017
Minor Update	August 2022
Next Review Date	June 2024
Approval Note	The Chief Security Officer has the authority to approve minor (but not material) revisions and amendments without the requirement for a repeat approval, under delegated authority of the General Manager IST.

Appendix I Glossary

Term	Definition
Information	All recorded forms of data, knowledge, facts, intentions, opinions or analysis, irrespective of the medium through which it is communicated or stored. Information may be contained in a variety of media, for example: printed documents, hand written notes, diaries, maps, spatial and photographic data, images, videos, electronic databases, electronic documents, emails, web pages, voice mail and audio records.
Structured information	Information that resides in the rows and columns of a database.
Unstructured information	Information that does not reside in the rows and columns of a database. Unstructured information comes in many forms, including word processing documents, spreadsheets, email, social media posts, and log files automatically generated by computer servers. Unstructured information does not always have a predetermined form, business purpose, use, value, or security classification.
Metadata	The data attached to a document or information item in order to manage, store, locate and dispose of it. Metadata describes content by capturing key data about the item and its context e.g. title, create date, creator, and version.
Public Record	A record created, or received, by a public office in the conduct of its affairs. Under the Act, all Transpower's information may be deemed to be Public Records.
Recordkeeping	The creation and maintenance of complete accurate and reliable evidence of business transactions in the form of recorded Information.
Retention and Disposal Schedule	A systematic listing of the records created by an organisation which plans the life of these records from creation to disposal and is agreed with Archives New Zealand and signed off by the Chief Archivist and the Chief Executive of Transpower.
Transpower Personnel	All employees, contractors, consultants and temporary resources working on Transpower's behalf.

Appendix 2: Guideline - Information Handling Table (NB this is ‘living document’ and will be subject to revision)

		PUBLIC	IN CONFIDENCE	SENSITIVE	RESTRICTED
All	**Documents**	Where applicable, ensure integrity of the information at point of dissemination	• All business documents must be classified and stored on authorised Transpower systems/devices. • Should, where practicable, be marked “IN CONFIDENCE” or “Transpower - IN CONFIDENCE” on every page.	• Must be clearly labelled “SENSITIVE” or “Transpower - SENSITIVE” and stored on appropriately secured Transpower systems/devices. • Must not be shared with unauthorised users.	• Must be clearly labelled “RESTRICTED” or “Transpower – RESTRICTED” and stored on appropriately secured Transpower systems/devices. • Must not be shared without explicit approval of the document owner.
Transfer	**Verbal discussions, Video displays, and transmission to Mobile devices**		• Personally owned devices must access Transpower information through Secure Remote Access and care must be taken to ensure that content is not visible to unauthorised individuals.	• Must not be exchanged when unauthorised individuals are in close proximity or would be able to overhear or be overseen on a device. • May (depending on its risk profile) be encrypted when in transit to mobile devices over untrusted networks.	• Must not be exchanged when unauthorised individuals are in close proximity or would be able to be overheard or be overseen on a device.
	Email		• Should, where practicable, be marked in the subject or body of message “IN CONFIDENCE“ or “Transpower – IN CONFIDENCE”. • Mobile devices must be password protected.	• Must be marked in the subject or body of the message “SENSITIVE” or “Transpower - SENSITIVE”. • Mobile devices must be password protected.	• Must not be transferred over a Public or 3rd party network unless part of an approved business process with the relevant risks accepted or mitigated using additional accepted security controls.
	Public IP Networks		• May (depending on its risk profile) be encrypted when transmitted across public networks.	• Must be encrypted when transmitted across public networks. • Overseas transfers of information require further risk assessment.	
	Fax		• Should, where practicable, be marked “IN CONFIDENCE” or “Transpower – IN CONFIDENCE	• Must not be sent by fax unless part of an approved business process that operates to mitigate the relevant risks. • Must be marked “SENSITIVE” or “Transpower - SENSITIVE”.on every page.	• RESTRICTED documents when posted must be double enveloped. • May be carried by ordinary postal services or commercial courier firms, provided the envelope/package is sealed and the word “RESTRICTED” is not visible. • The outer envelope must clearly show a return address in case delivery is unsuccessful—a return PO Box number would suffice. • The outer envelope should be addressed to an individual by name and title.
	Hard copy		• No special handling requirements.	• Must be delivered by Transpower employee or a tracked service unless part of an approved business process that operates to mitigate the relevant risks.	
Storage	**Mobile devices**		• Mobile devices must be password protected.	• Transpower commercial and personally identifying information must be protected by two-factor authentication when stored on mobile devices. • Mobile devices must be password protected and remain in the individual’s personal possession and control. • Mobile devices need to have approved hard drive encryption software deployed to them.	• Must not be stored on a mobile device unless part of an approved business process with the relevant risks accepted or mitigated using additional accepted security controls.

	Public Storage Providers / 3rd Parties		• Must be protected by two-factor authentication if accessible from a Public IP based location.	• Must be protected by two factor authentication if accessible from a Public IP-based location.	• RESTRICTED information must not be stored on Public or 3rd party storage location unless part of an approved business process with the relevant risks accepted or mitigated using additional accepted security controls.
	Non-Portable media		• Transpower's technical security controls are designed to protect information automatically. • External storage devices should be password protected.	• Transpower's technical security controls are designed to protect information automatically. • External storage devices should be password protected or encrypted.	• Transpower's technical security controls are designed to protect information automatically. • External storage devices should be password protected or encrypted.
	Hard copy		• Should, where practicable, be marked "IN CONFIDENCE" or "Transpower - IN CONFIDENCE" on every page.	• Must be locked away in filing cabinets, credenzas, or closets and care must be taken to ensure it cannot be overseen. • Must be marked "SENSITIVE" or "Transpower - SENSITIVE" on every page.	• Must be locked away in filing cabinets, credenzas, or closets and care must be taken to ensure it cannot be overseen. • Must be marked "RESTRICTED" or "Transpower – RESTRICTED" on every page.
Disposal	**Hard copy and electronic media**		• Must ONLY be done in accordance with the Disposal Schedule as approved by the Chief Archivist (Archives NZ). • Must be disposed of by a secure process within the Transpower (e.g. shredding) or contracted out with the relevant requirements set out in the contractual arrangements (e.g. secure disposal bins). • Must be in accordance with Media Sanitisation and Decommissioning processes.	• Must ONLY be done in accordance with the Disposal Schedule as approved by the Chief Archivist (Archives NZ). • Must be disposed of by a secure process within the Transpower (e.g. shredding) or contracted out with the relevant requirements set out in the contractual arrangements (e.g. secure disposal bins). • Must be disposed of in a way that makes reconstruction highly unlikely, such as mechanical shredding.	• Must ONLY be done in accordance with the Disposal Schedule as approved by the Chief Archivist (Archives NZ) • Must be disposed of by a secure process within the Transpower (e.g. shredding) or contracted out with the relevant requirements set out in the contractual arrangements (e.g. secure disposal bins). • Must be disposed of in a way that makes reconstruction highly unlikely, such as mechanical shredding.
	Public Storage Providers / 3rd Parties		• Must ONLY be done in accordance with the Disposal Schedule as approved by the Chief Archivist (Archives NZ). • Must be assured that the Public Storage Provider / 3rd Party disposes in accordance to best practises for electronic media sanitisation.	• Must ONLY be done in accordance with the Disposal Schedule as approved by the Chief Archivist (Archives NZ). • Must be assured that the Public Storage Provider / 3rd Party disposes in accordance to best practises for electronic media sanitisation of SENSITIVE data in a way that makes restoration highly unlikely, such as overwriting data with zeroes before deletion.	• Must ONLY be done in accordance with the Disposal Schedule as approved by the Chief Archivist (Archives NZ). • Must be assured that the Public Storage Provider / 3rd Party disposes in accordance to best practises for electronic media sanitisation of RESTRICTED data in a way that makes restoration highly unlikely, such as overwriting data with zeroes before deletion.

Notes relating to Information Handling Table

1. Mobile devices include such technology as laptops, notebooks, tablets, smartphones and USBs.
2. Non-portable media include Transpower desktops and Storage Area Networks (SAN).
3. The focus of this table is on information handling. Refer to:
   a. Security Awareness & Appropriate Usage Policy for information on mandated storage methods.
   b. ICT Boundary Defence Standard for information on remote access.
4. Any classifications attached to emails will, where practicable, be added from the source system of the email. For example, if a source system was classified as SENSITIVE it would add a SENSITIVE classification to any emails coming out of it.