GUIDELINES FOR PROTECTION OF OFFICIAL INFORMATION

www.security.govt.nz

SELECTING AN APPROPRIATE SECURITY CLASSIFICATION

Official Information Act 1982

The Official Information Act allows information to be protected to the extent consistent with the public interest and the preservation of personal privacy. Classifications are used to grade information on the basis of the damage that would result from unauthorised disclosure and to specify the protective measures to be applied. In themselves, classifications do not allow official information to be withheld; rather, the information must be considered on its merits using the criteria in the Act.

Endorsements: May be applied in front of any security classification

APPOINTMENTS : BUDGET : CABINET : COMMERCIAL : EVALUATIVE : HONOURS : MEDICAL : STAFF : POLICY : NEW ZEALAND EYES ONLY : [DEPARTMENT(S)] USE ONLY: ADDRESSEE ONLY : EMBARGOED FOR RELEASE : TO BE REVIEWED ON

NATIONAL SECURITY

Compromise would damage the security, defence or international relations of New Zealand and/or friendly governments

POLICY AND PRIVACY

Compromise would damage the functions of government, or cause loss (privacy, safety, commercial) to a person

TOP SECRET — Damage national interests in an exceptionally grave manner

- Directly threaten the internal stability of NZ or friendly countries
- Lead directly to widespread loss of life
- Cause exceptional damage to the security of NZ forces or allies
- Cause exceptional damage to the operational effectiveness of NZ forces or friendly forces
- Cause exceptional damage to the continuing effectiveness of extremely valuable security or intelligence operations
- Cause exceptional damage to relations with other governments
- Cause severe long term damage to significant national infrastructure

SECRET — Damage national interests in a serious manner

- Raise international tension
- Seriously damage relations with friendly governments
- Seriously damage the security of NZ forces or friendly forces
- Seriously damage the operational effectiveness of NZ forces or friendly forces
- Seriously damage the effectiveness of valuable security or intelligence operations
- Seriously damage the internal stability of NZ or friendly countries
- Shut down or substantially disrupt significant national infrastructure

CONFIDENTIAL — Damage national interests in a significant manner

- Materially damage diplomatic relations— cause formal protest or other sanctions
- Damage the operational effectiveness of NZ forces or friendly forces
- Damage the security of NZ forces or friendly forces
- Damage the effectiveness of valuable security or intelligence operations
- Damage the internal stability of NZ or friendly countries
- Disrupt significant national infrastructure

RESTRICTED — Adversely affect national interests

- Adversely affect diplomatic relations
- Hinder operational effectiveness of NZ forces or friendly forces
- Hinder security of NZ forces or friendly forces
- Adversely affect internal stability of NZ or friendly countries
- Adversely affect economic well-being of NZ or friendly countries

SENSITIVE — Damage Govt interests, endanger citizens

- Endanger the safety of any person
- Seriously damage the economy of NZ
- Impede Govt negotiations

IN-CONFIDENCE — Prejudice law & order, impede Govt business, affect citizen privacy

- Prejudice maintenance of the law
- Adversely affect privacy of a natural person
- Prejudice citizen's commercial information
- Prejudice obligations of confidence
- Prejudice measures that protect the health or safety of the public
- Prejudice economic interests of NZ
- Prejudice measures that prevent or mitigate material loss to the public
- Breach constitutional conventions
- Impede the effective conduct of public affairs
- Breach legal professional privilege
- Impede Govt commercial activities
- Disclosure or use of information for improper gain or advantage

HANDLING and/or TRANSMITTING POLICY AND PRIVACY INFORMATION

RESTRICTED and SENSITIVE

Principles and Clearance Levels

- Information classified as RESTRICTED or SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely.
- Only staff authorised by the Department to access RESTRICTED or SENSITIVE levels are to handle this type of information. This includes all staff involved with transmission, storage, and disposal.

Electronic Transmission

- Information must be marked RESTRICTED or SENSITIVE.
- All RESTRICTED or SENSITIVE information transmitted across public networks (this includes the Internet) within NZ or across any networks overseas must be encrypted using a system approved by GCSB.

Note: Your Departmental Security Officer will provide details on what encryption systems are available.

Electronic Storage

- Electronic files must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms:
  - User challenge and authentication
  - Logging use at level of individual
  - Firewalls and intrusion detection systems and procedures
  - Server authentication
  - OS-specific/ application-specific security measures
  - Encryption

Electronic Disposal

- Electronic files, magnetic and other storage media should be disposed of in a way that makes reconstruction highly unlikely.
- The information may be destroyed by using the delete function.
- If media is to be disposed of or sold, it must be purged using a GCSB approved secure delete facility or physically destroyed.

Paper Transmission

- RESTRICTED and SENSITIVE 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 or SENSITIVE 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.
- RESTRICTED and SENSITIVE mail for/from overseas should be carried by diplomatic airfreight by MFAT.

Paper Storage

- RESTRICTED and SENSITIVE documents should be stored in compliance with Archives NZ Storage Standard NAS 9901 *Storage of Public Records or Archives.*

Paper Waste Disposal

- Must comply with provisions of Archives Act 1957
- RESTRICTED and SENSITIVE documents are to be disposed of or destroyed in a way that makes reconstruction highly unlikely, such as mechanical shredding.

IN-CONFIDENCE

Principles and Clearance Level

- Information for official use, with consideration of "need to know" principle.

Electronic Transmission

- Information must be marked IN-CONFIDENCE.
- IN-CONFIDENCE data can be transmitted across external or public networks (including the Internet) without being encrypted. The level of information contained should be assessed before transmitting.
- Username/Password access control and/or encryption should be considered.
- All IN-CONFIDENCE information (including data) is to clearly identify the originating Govt agency and data.
- An appropriate statement should accompany all IN-CONFIDENCE information transmitted via e-mail or Fax.

Electronic Storage

- Electronic files should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms:
  - User challenge and authentication
  - Logging use at level of individual
  - Firewalls and intrusion detection systems and procedures
  - Server authentication
  - OS-specific/ application-specific security measures

Electronic Disposal

- Electronic files, magnetic and other storage media should be disposed of in a way that makes compromise highly unlikely.
- The information may be destroyed by using the delete function.
- If media is to be disposed of or sold, it must be purged using a GCSB approved secure delete facility or physically destroyed.

Paper Transmission

- IN-CONFIDENCE documents may be posted in a single 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 of delivery is unsuccessful—a return PO Box number would suffice.

Paper Storage

- IN-CONFIDENCE documents can be secured using the normal building security and door-swipe card systems that aim to simply keep the public out of the administration areas.

Paper Waste Disposal

- Must comply with provisions of Archives Act 1957
- IN-CONFIDENCE documents are to be disposed of in a way that makes compromise highly unlikely, such as depositing the documents in bins that are taken away for secure destruction.

HANDLING and/or TRANSMITTING TOP SECRET, SECRET and CONFIDENTIAL

— refer to Manual *"Security In Government Departments"* (SIGD)