



GUIDELINES FOR PROTECTION OF OFFICIAL INFORMATION



SELECTING AN APPROPRAITE SECURITY CLASSIFICATION

HANDLING and/or TRANSMITTING POLICY AND PRIVACY INFORMATION

National Security Classifications

Policy and Privacy Classifications

Information, for which compromise could affect the security or defence of New Zealand or the international relations of the Government of New Zealand

Information, for which compromise does not threaten the security of the nation, but rather the security or interests of individuals, groups, commercial entities, government business and the community

SENSITIVE

Compromise of information would be likely to damage the interests of New Zealand or endanger the safety of its citizens

- Endanger the safety of any person.
- Damage seriously the economy of New Zealand by disclosing prematurely decisions to change or continue Government economic or financial policies relating to:
 - exchange rates or the control of overseas exchange transactions
 - the regulation of banking or credit
 - taxation
 - the stability, control, and adjustment of prices of goods and services, rents and other costs, and rates of wages, salaries and other incomes
 - the borrowing of money by the Government of New Zealand
 - the entering into of overseas trade agreements.
- Impede a Minister of the Crown or a department organisation holding the information to carry on without prejudice or disadvantage, negotiations (including commercial and industrial negotiations).

IN-CONFIDENCE

Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens.

- Prejudice the maintenance of law, including the prevention, investigation and detection of offences, and the right to a fair trial.
- Affect adversely the privacy of natural persons, including that of deceased natural persons.
- Disclose a trade secret or unreasonably to prejudice the commercial position of the person who supplied or is the subject of the information.
- Prejudice measures protecting the health or safety of members of the public.
- Prejudice the substantial economic interests of New Zealand.
- Prejudice measures that prevent or mitigate material loss to members of the public.
- Breach legal professional privilege.
- Impede a Minister of the Crown or any Department or organisation holding the information to carry out, without prejudice or disadvantage, commercial activities.
- Lead to the disclosure or use of official information for improper gain or advantage.
- Disclose information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied; or be likely otherwise to damage the public interest.
- Breach the constitutional conventions for the time being which protect: the confidentiality of communications by or with the Sovereign or Her representative; collective and individual ministerial responsibility; the political neutrality of officials; and the confidentiality of advice tendered by ministers of the Crown and officials.
- Impede the effective conduct of public affairs through: the free and frank expression of opinion by or between or to Ministers of the Crown or officers and employees of any department or organisation in the course of their duty; the protection of such Ministers, officers and employees from improper pressure or harassment.

TOP SECRET

Compromise of information would 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 exceptionally grave damage to the operational effectiveness or security of New Zealand or friendly forces or the effectiveness of extremely valuable security or intelligence operations
- Cause extremely grave damage to relations with other governments
- Cause severe long-term damage to significant national infrastructure

SECRET

Compromise of information would damage national interests in a serious manner

- Raise international tension
- Damage seriously relations with friendly governments
- Cause serious damage to the operational effectiveness or security of New Zealand or friendly or the effectiveness of valuable security or intelligence operations
- Seriously damage the internal stability of New Zealand or friendly countries
- Shut down or substantially disrupt significant, national infrastructure

CONFIDENTIAL

Compromise of information would damage national interests in a significant manner

- Materially damage diplomatic relations (i.e. cause formal protest or other sanctions)
- Cause damage to the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of valuable security or intelligence operations
- Damage the internal stability of New Zealand or friendly countries
- Disrupt significant national infrastructure

RESTRICTED

Compromise of information would be likely to affect the national interests in an adverse manner

- Affect diplomatic relations adversely
- Hinder operational effectiveness of New Zealand or friendly forces
- Hinder security of NZ forces or friendly forces
- Affect the internal stability or economic well-being of New Zealand or friendly countries adversely

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 authorised to handle the information. This includes all staff involved with transmission, storage, and disposal.

Electronic Transmission

- All RESTRICTED or SENSITIVE information transmitted across public networks within New Zealand or across any networks overseas must be encrypted using a system approved by GCSB.

Electronic Storage

- Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms:
 - user challenge and authentication (username/password or digital ID/Certificate)
 - 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 should be disposed of in a way that makes reconstruction highly unlikely.

Manual Transmission

- **Within a single physical location.** As determined by the Chief Executive or Head of the organisation.
- **Transfer between establishments within or outside New Zealand.**
 - May be carried by ordinary postal service or commercial courier firms, provided the envelope/package is closed and the word RESTRICTED or SENSITIVE is not visible.
 - The outer envelope should be addressed to an individual by name and title. RESTRICTED/SENSITIVE mail for/from Overseas posts should be carried by diplomatic airfreight via MFAT.
 - The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.

Manual Storage

- In an office environment, RESTRICTED and SENSITIVE material should be held in a lockable storage area or cabinet.
- In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.

Manual Disposal

- RESTRICTED and SENSITIVE documents are to be disposed of or destroyed in a way that makes reconstruction highly unlikely.

IN-CONFIDENCE

Principle and Clearance Level

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

Electronic Transmission

- An appropriate statement should accompany all IN CONFIDENCE information transmitted via e-mail or fax.
- It should outline legal responsibilities and notification/destruction instructions if the incorrect party receives it.
- IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text.
- Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in public agencies).
- All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.

Electronic Storage

- Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms:
 - user challenge and authentication (username/password or digital ID/Certificate)
 - 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 should be disposed of in a way that makes reconstruction highly unlikely.

Manual Transmission

- May be carried by ordinary postal service or commercial courier firm as well as mail delivery staff in a single closed envelope.
- The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.

Manual Storage

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

Manual Disposal

- Disposed of by departmental arrangements.

ENDORSEMENTS (may be used with 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

FOR FURTHER INFORMATION REFER TO:
WWW.PROTECTIVESECURITY.GOV.TZ



GUIDELINES FOR PROTECTION OF OFFICIAL INFORMATION

HANDLING and/or TRANSMITTING PROTECTIVELY MARKED NATIONAL SECURITY INFORMATION

CONFIDENTIAL	SECRET	TOP SECRET
<p style="text-align: center;">Principles and Clearance Levels</p> <ul style="list-style-type: none"> Information classified as CONFIDENTIAL must be held, processed, transmitted and destroyed with levels of security commensurate with the significant damage to national security that compromise would incur. Only Staff cleared by the department for CONFIDENTIAL access or above is authorised to handle the information. This includes all staff involved with transmission, storage, and disposal. 	<p style="text-align: center;">Principles and Clearance Levels</p> <ul style="list-style-type: none"> Information classified as SECRET must be held, processed, transmitted and destroyed with levels of security commensurate with the serious damage to national security that compromise would incur. Only Staff cleared by the department for SECRET access or above is authorised to handle the information. This includes all staff involved with transmission, storage, and disposal. 	<p style="text-align: center;">Principles and Clearance Levels</p> <ul style="list-style-type: none"> Information classified as TOP SECRET must be held, processed, transmitted and destroyed with levels of security commensurate with the exceptionally grave damage to national interest that compromise would incur. Only staff cleared by the department for TOP SECRET access is authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
<p style="text-align: center;">Electronic Transmission</p> <ul style="list-style-type: none"> All CONFIDENTIAL information transmitted across any networks within New Zealand or overseas must be encrypted using a system approved and accredited by GCSB. 	<p style="text-align: center;">Electronic Transmission</p> <ul style="list-style-type: none"> All SECRET information transmitted across any networks within New Zealand or overseas must be encrypted using a system approved and accredited by GCSB. 	<p style="text-align: center;">Electronic Transmission</p> <ul style="list-style-type: none"> All TOP SECRET information transmitted across any network within New Zealand or overseas must be encrypted using a system approved and accredited by the GCSB.
<p style="text-align: center;">Electronic Storage</p> <ul style="list-style-type: none"> Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through the judicious selection of two or more of the following mechanisms: <ul style="list-style-type: none"> - user challenge and authentication (username/password or digital ID/Certificate) - logging use at level of individual - firewalls and intrusion-detection systems and procedures; server authentication - OS-specific/application-specific security measures 	<p style="text-align: center;">Electronic Storage</p> <ul style="list-style-type: none"> Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through the judicious selection of two or more of the following mechanisms: <ul style="list-style-type: none"> - user challenge and authentication (username/password or digital ID/Certificate) - logging use at level of individual - firewalls and intrusion-detection systems and procedures; server authentication - OS-specific/application-specific security measures 	<p style="text-align: center;">Electronic Storage</p> <ul style="list-style-type: none"> Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through the judicious selection of two or more of the following mechanisms: <ul style="list-style-type: none"> - user challenge and authentication (username/password or digital ID/Certificate) - logging use at level of individual - firewalls and intrusion-detection systems and procedures; server authentication - OS-specific/application-specific security measures
<p style="text-align: center;">Electronic Disposal</p> <ul style="list-style-type: none"> Media that has held CONFIDENTIAL information must be declassified by degaussing, overwriting or destroying iaw GCSB guidelines contained in chapter 12.6 of the <i>NZISM</i>. 	<p style="text-align: center;">Electronic Disposal</p> <ul style="list-style-type: none"> Media that has held SECRET information must be declassified by degaussing, overwriting or destroying iaw GCSB guidelines contained in chapter 12.6 of the <i>NZISM</i>. 	<p style="text-align: center;">Reproduction</p> <ul style="list-style-type: none"> All TOP SECRET information must be made ACCOUNTABLE MATERIAL by default. Once disseminated, ACCOUNTABLE MATERIAL must not be copied or reproduced in any form. If additional copies are required, they must be requested from the original source.
<p style="text-align: center;">Manual Transmission</p> <ul style="list-style-type: none"> Within a single physical location. Single opaque envelope that indicates the classification, with receipt at the discretion of the originator, and either: <ul style="list-style-type: none"> - despatched through department's own transit system; or - distributed within a building or part of a building that has been declared a specially protected area; otherwise - must be double enveloped and sealed with approved seals in accordance with PSR - <i>Handling Requirements for Protectively Marked Information and Equipment</i> and carried by authorised, sufficiently security vetted messengers. Transfer between establishments within New Zealand. CONFIDENTIAL material should be double enveloped and sealed with approved seals in accordance with PSR - <i>Handling Requirements for Protectively Marked Information and Equipment</i> and: <ul style="list-style-type: none"> - carried by an authorised messenger or safe-hand courier with "By Hand" stamped on the outer envelope, or - When no authorised messenger or safe-hand courier service exists CONFIDENTIAL material may be sent by signature required commercial courier or registered post. Receipts must be retained. Transfer between establishments outside New Zealand. Confidential material must be double enveloped with "By Hand" stamped on the outer envelope and sealed with approved seals in accordance with PSR - para 6.1 <i>Handling Requirements for Protectively Marked Information and Equipment</i> with a receipt form included inside the inner envelope and: <ul style="list-style-type: none"> - carried by Diplomatic safe-hand bag service operated by MFAT to or between posts; or - where no safe-hand courier service exists material may be sent by registered post within Australia, Canada, and the United States of America between New Zealand posts situated in respective countries; or - in exceptional circumstances CONFIDENTIAL material may be transmitted by registered mail between New Zealand diplomatic posts or other New Zealand agencies situated in the United Kingdom, Canada, Australia and the United States of America, or by Diplomatic air freight bag between MFAT and New Zealand official missions in Niue and Tarawa. For further advice contact NZSIS. COMSEC material. To be handled as stated in the Physical Security Management protocol of PSR 	<p style="text-align: center;">Manual Transmission</p> <ul style="list-style-type: none"> Within a single physical location. Material should be double enveloped and sealed in accordance with PSR - <i>Handling Requirements for Protectively Marked Information and Equipment</i> and: <ul style="list-style-type: none"> - despatched through a department's own transit system with hand-to-hand receipts at each stage of the journey; or - distributed within a building or part of a building that has been declared a specially protected area; otherwise - carried by authorised messengers. Transfer between establishments within New Zealand. SECRET material must be double enveloped and sealed with approved seals in accordance with PSR - <i>Handling Requirements for Protectively Marked Information and Equipment</i> and carried by authorised, sufficiently security vetted messengers or safe-hand courier. Transfer between establishments outside New Zealand. SECRET material must be double enveloped and sealed with approved seals in accordance with PSR - <i>Handling Requirements for Protectively Marked Information and Equipment</i> with a receipt form included inside the inner envelope and carried by Diplomatic safe-hand bag service operated by MFAT. COMSEC material. To be handled as stated in the Physical Security Management protocol of PSR 	<p style="text-align: center;">Electronic Disposal</p> <ul style="list-style-type: none"> Media that has held TOP SECRET information cannot be declassified and must be destroyed iaw GCSB guidelines contained in chapter 12.6 of the <i>NZISM</i>. <p style="text-align: center;">Manual Transmission</p> <ul style="list-style-type: none"> Within a single physical location. Material must be double enveloped and sealed with approved seals in accordance with PSR - <i>Handling Requirements for Protectively Marked Information and Equipment</i> and carried by authorised, sufficiently security vetted messengers <ul style="list-style-type: none"> - dispatched through a department's own transit system with hand-to-hand receipts at each stage of the journey; or - distributed within a building or part of a building that has been declared a specially protected area (SCIF); otherwise - carried by authorised messengers within an NZSIS approved circulating box or pouch. Transfer between establishments within New Zealand. TOP SECRET material must be double enveloped and sealed with approved seals in accordance with PSR - <i>Handling Requirements for Protectively Marked Information and Equipment</i> and carried by authorised, sufficiently security vetted messengers Transfer between establishments outside New Zealand. TOP SECRET material must be double enveloped and sealed with approved seals in accordance with PSR - <i>Handling Requirements for Protectively Marked Information and Equipment</i> with a receipt form included inside the inner envelope and carried by the Diplomatic safe-hand bag service operated by MFAT. COMSEC material. To be handled as stated in the Physical Security Management protocol of PSR
<p style="text-align: center;">Manual Storage</p> <ul style="list-style-type: none"> Must be locked in an approved security container when not in use. See PSR - Table 5 of para 4.12 of Security zones and risk mitigation in the Physical security management protocols The minimum acceptable storage arrangements are a combination of the protection afforded by the security container itself, the position or site and the use of approved security equipment. 	<p style="text-align: center;">Manual Storage</p> <ul style="list-style-type: none"> Must be locked in an approved security container when not in use. See PSR - Table 5 of para 4.12 of Security zones and risk mitigation in the Physical security management protocols. The minimum acceptable storage arrangements are a combination of the protection afforded by the security container itself, the position or site (Security Zone) and the use of approved security equipment. 	<p style="text-align: center;">Manual Storage</p> <ul style="list-style-type: none"> Must be locked in an approved security container when not in use. See PSR - Table 5 of para 4.12 of Security Zones and Risk Mitigation in the Physical security management protocols The minimum acceptable storage arrangements are a combination of the protection afforded by the security container itself, the position or site (Security Zone) and the use of approved security equipment.
<p style="text-align: center;">Manual Disposal</p> <ul style="list-style-type: none"> If accountable, the destruction should be recorded by marking the record of accountable documents or the file index sheet where these are used. See PSR Section 9 of <i>Handling Requirements for Protectively Marked Information and Equipment</i> Destroy by burning, pulping, shredding or dry maceration. 	<p style="text-align: center;">Manual Disposal</p> <ul style="list-style-type: none"> If accountable, the destruction should be recorded by marking the record of accountable documents or the file index sheet where these are used. See PSR Section 9 of <i>Handling Requirements for Protectively Marked Information and Equipment</i> Destroy by burning, pulping, shredding or dry maceration. 	<p style="text-align: center;">Manual Disposal</p> <ul style="list-style-type: none"> Before destruction all pages and enclosures must be verified as present. The destruction must be supervised and witnessed and should be recorded by filing a note of destruction in the place of the document or by marking the relevant entry on the file index sheet where these are authorised. See PSR Section 9 of <i>Handling Requirements for Protectively Marked Information and Equipment</i> Destroy by burning, pulping, shredding or dry maceration.

**FOR FURTHER INFORMATION REFER TO:
WWW.PROTECTIVESECURITY.GOV.TZ**

National Security Clearance Indicators

- A- = CONFIDENTIAL
- A = SECRET
- B = TOP SECRET
- B = TOP SECRET SPECIAL

GUIDELINES FOR PROTECTION OF OFFICIAL INFORMATION

POLICY AND PRIVACY PROTECTIVE MARKINGS

Information, for which compromise does not threaten the security of the nation, but rather the security or interests of individuals, groups, commercial entities, government business and the community

SENSITIVE

Compromise of information would be likely to damage the interests of New Zealand or endanger the safety of its citizens

- # Endanger the safety of any person
- # Damage seriously the economy of New Zealand by disclosing prematurely decisions to change or continue Government economic or financial policies relating to:
 - exchange rates or the control of overseas exchange transactions
 - the regulation of banking or credit
 - taxation
 - the stability, control, and adjustment of prices of goods and services, rents and other costs, and rates of wages, salaries and other incomes
 - the borrowing of money by the Government of New Zealand
 - the entering into of overseas trade agreements
- # Impede a Minister of the Crown or a department organisation holding the information to carry on without prejudice or disadvantage, negotiations (including commercial and industrial negotiations)

IN-CONFIDENCE

Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens

- # Prejudice the maintenance of law, including the prevention, investigation and detection of offences, and the right to a fair trial.
- # Affect adversely the privacy of natural persons, including that of deceased natural persons.
- # Disclose a trade secret or unreasonably to prejudice the commercial position of the person who supplied or is the subject of the information.
- # Prejudice measures protecting the health or safety of members of the public.
- # Prejudice the substantial economic interests of New Zealand.
- # Prejudice measures that prevent or mitigate material loss to members of the public.
- # Breach legal professional privilege.
- # Impede a Minister of the Crown or any Department or organisation holding the information to carry out, without prejudice or disadvantage, commercial activities.
- # Lead to the disclosure or use of official information for improper gain or advantage.
- # Disclose information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied; or be likely otherwise to damage the public interest.
- # Breach the constitutional conventions for the time being which protect:
 - the confidentiality of communications by or with the Sovereign or Her representative;
 - collective and individual ministerial responsibility;
 - the political neutrality of officials; and
 - the confidentiality of advice tendered by ministers of the Crown and officials.
- # Impede the effective conduct of public affairs through:
 - the free and frank expression of opinion by or between or to Ministers of the Crown or officers and employees of any department or organisation in the course of their duty;
 - the protection of such Ministers, officers and employees from improper pressure or harassment.

FOR FURTHER INFORMATION REFER TO:

WWW.PROTECTIVESECURITY.GOV.TZ

MARKING OFFICIAL INFORMATION

PROTECTIVE MARKING HERE

Document Marking

1. For all documents the proper method of displaying the protective marking (TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, *TOPIC-SENSITIVE*, *TOPIC-IN-CONFIDENCE* or even UNCLASSIFIED) is in **BOLD** capitals as **header** and **footer** on each page, i.e. the very top and bottom of each page

2. For UNCLASSIFIED documents, you only need to mark the document if it is handled along with other documents that are of a National Security, Policy or Privacy type.

PROTECTIVE MARKING HERE

From: Joe Bloggs
Date: 5/5/XX 14:02:23
To: Bill Smith
Subject: (**PROTECTIVE MARKING HERE**) Subject
Displaying protective markings on Emails

For an email, the Protective marking of RESTRICTED, *TOPIC-SENSITIVE*, *TOPIC-IN-CONFIDENCE* or even UNCLASSIFIED is in **BOLD** capitals the front of the subject.

Do not send TOP SECRET, SECRET or CONFIDENTIAL information by email (Unless GCSB has approved/ accredited the system you use).

If you print out an email that displays a protective marking, *handwrite* or *rubber stamp* the marking in the footer and header of each page.

If there is no Protective Marking on the document or email, before assuming it is UNCLASSIFIED, read it to assess what type of information it is and, if need be, mark and handle as required to avoid compromise. Notify or discuss your opinion with the originator.

NATIONAL SECURITY PROTECTIVE MARKINGS

Information, for which compromise could affect the security or defence of New Zealand or the international relations of the Government of New Zealand

TOP SECRET

Compromise of information would damage national interests in an exceptionally grave manner

- ! Directly threatens the internal stability of NZ or friendly countries
- ! Leads directly to widespread loss of life
- ! Causes exceptionally grave damage to the operational effectiveness or security of New Zealand or friendly forces or the effectiveness of extremely valuable security or intelligence operations
- ! Causes extremely grave damage to relations with other governments
- ! Causes severe long-term damage to significant national infrastructure

SECRET

Compromise of information would damage national interests in a serious manner

- ! Raises international tension
- ! Seriously damages relations with friendly governments
- ! Causes serious damage to the operational effectiveness or security of New Zealand or friendly or the effectiveness of valuable security or intelligence operations
- ! Seriously damages the internal stability of New Zealand or friendly countries
- ! Shuts down or substantially disrupts significant, national infrastructure

CONFIDENTIAL

Compromise of information would damage national interests in a significant manner

- ! Materially damages diplomatic relations (i.e. cause formal protest or other sanctions)
- ! Causes damage the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of valuable security or intelligence operations
- ! Damages the internal stability of New Zealand or friendly countries
- ! Disrupts significant national infrastructure

RESTRICTED

Compromise of information would be likely to affect the national interests in an adverse manner

- ! Affects diplomatic relations adversely
- ! Hinders operational effectiveness of New Zealand or friendly forces
- ! Hinders security of NZ forces or friendly forces
- ! Affects the internal stability or economic well-being of New Zealand or friendly countries adversely

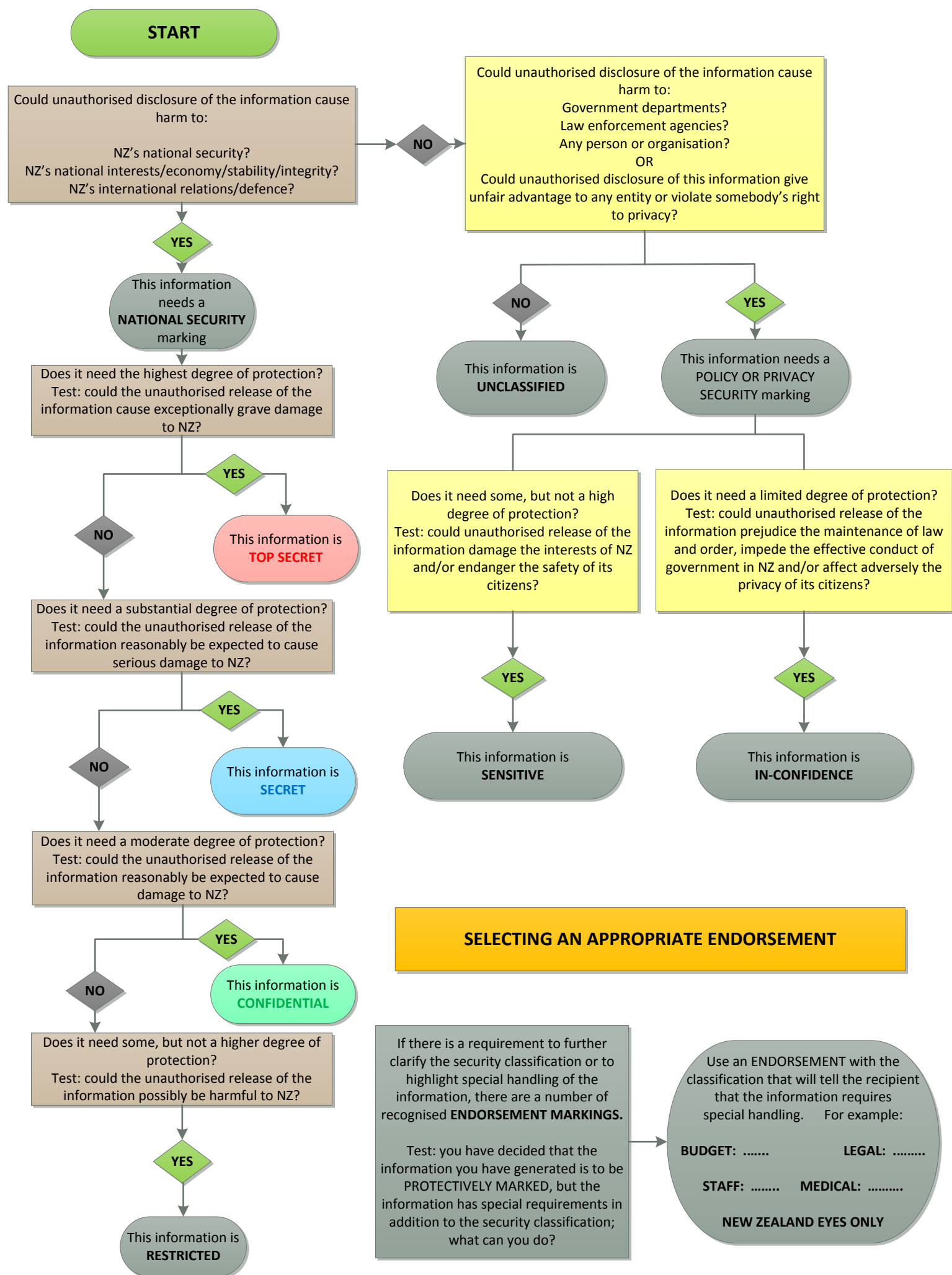
ENDORSEMENTS

(may be used with any security classification)

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

SELECTING AN APPROPRIATE SECURITY CLASSIFICATION - FOR FURTHER INFORMATION REFER TO THE:

**Protective Security Requirements (PSR) - Information Security Management Protocol
Handling Requirements for Protectively Marked Information and Equipment**



FOR FURTHER INFORMATION REFER TO:
WWW.PROTECTIVESECURITY.GOV.T.NZ

ACCOUNTABLE MATERIAL	The ACCOUNTABLE MATERIAL endorsement marking is used to indicate that the information requires strict control over access to, and movement of, as well as regular auditing to ensure its safe custody. What constitutes ACCOUNTABLE MATERIAL will vary from agency to agency. A risk assessment will determine the frequency of auditing practices. Note: TOP SECRET information is ACCOUNTABLE MATERIAL by default.
APPOINTMENTS	The APPOINTMENTS endorsement marking may be used when actual or potential appointments have not yet been announced or for the deliberation during the recommendation/approval process.
BUDGET	The BUDGET endorsement marking may be used for proposed or actual measures for the Budget prior to their announcement.
CABINET	The CABINET endorsement marking may be used for material that will be presented to, and/or require decisions by, Cabinet or Cabinet Committee.
COMMERCIAL	The COMMERCIAL endorsement marking may be used for commercially sensitive processes, negotiations or affairs.
[DEPARTMENT] USE ONLY	The [DEPARTMENT(S)] USE ONLY endorsement marking may be used for material intended only for use within the specified department(s).
EMBARGOED FOR RELEASE	The EMBARGOED FOR RELEASE endorsement marking may be used on material prior to a designated time at which an announcement or address will be made or the information will be disseminated.
EVALUATIVE	The EVALUATIVE endorsement marking may be used for material relating to competitive evaluations such as interview records and tender assessments.
HONOURS	The HONOURS endorsement marking may be used for material relating to the actual or potential award of an honour. It may be used before the announcement of the award and the deliberations during the recommendation or approval process or the consideration of honours policy matters involving the exercise of the royal prerogative.
LEGAL PRIVILEGE	The LEGAL PRIVILEGE endorsement marking may be used for material that is subject to legal privilege.
MEDICAL	The MEDICAL endorsement marking may be used for material relating to medical reports, records and other material related to them
NEW ZEALAND EYES ONLY (NZE0)	The NEW ZEALAND EYES ONLY (NZE0) endorsement marking indicates that access to information is restricted to appropriately security cleared New Zealand citizens on a need-to-know basis. For official information carrying the endorsement marking NZEO and the security classification IN CONFIDENCE, SENSITIVE or RESTRICTED, if an agency head considers that foreign nationals should be given information to which the endorsement marking NZEO applies, the agency head must consult with the originating agency to see if the endorsement marking is still required or whether it could be modified to enable release. It may be possible to have the endorsement marking removed or to release part of the information by removing the endorsement marking. For official information carrying the endorsement marking NZEO and the security classification CONFIDENTIAL, SECRET or TOP SECRET, foreign nationals must not be allowed access to NZEO information, even if they have the appropriate New Zealand security clearance. In limited circumstances, agencies may allow information marked NZEO to be viewed by appropriately cleared foreign nationals where there is an essential business need. In all such circumstances , the Director of Security, NZSIS must grant approval for this access.
STAFF	The STAFF endorsement marking may be used for material containing references to named or identifiable staff. Also for use by staff in entrusting personal confidences to management.
POLICY	The POLICY endorsement marking may be used for material relating to proposals for new or changed government policy before publication.
TO BE REVIEWED ON	The TO BE REVIEWED ON endorsement marking may be used where the classification is to be reviewed at the designated time.
RELEASEABLE TO (REL)	The RELEASEABLE TO or REL endorsement marking identifies information that has been released or is releasable to the indicated foreign countries or citizens of those indicated countries only. For example, RELEASABLE TO // GBR, NZ or REL // GBR, NZ means that the information may be passed to citizens and the governments of the United Kingdom and New Zealand only. It is common practice to put the countries in alphabetical order, with the originating country first. For example, RELEASABLE TO // NZ, CAN, GBR indicates that the originating country is New Zealand and the document can be shared with citizens and the governments of Canada and the United Kingdom.