Classification Handbook

Guidelines for protecting New Zealand Government information

PSR | Protective Security Requirements

Te Kāwanatanga o Aotearoa
New Zealand Government

Personal responsibility

Everyone who works with government (including staff, contractors and suppliers) has a personal responsibility and duty of care to safeguard the confidentiality, integrity, and availability of New Zealand Government information and assets that they use.

Accidental or deliberate compromise, loss or misuse of New Zealand Government information or assets is a security incident and may lead to damage or harm.

We must learn from security incidents to prevent or reduce the likelihood of future incidents. Repeated poor security behaviour and non-compliance with security policies can lead to disciplinary action, or in serious cases, to criminal prosecution.

Why classification matters

All government information requires an appropriate degree of protection depending on its level of sensitivity. By classifying government information and assets, you are clearly stating the sensitivity of the information or asset and reminding everyone of their obligations to keep it secure.

Benefits for you

- Classification lets you and others know how to correctly handle and protect government information and equipment.
- The appropriate use of classification helps to keep you safe, and your personal information protected from compromise.

Benefits for your organisation

- Classifying correctly will help your agency to reduce the risk of information security and privacy breaches.

Benefits for New Zealand Government

- Appropriate classification makes it easier to share information which agencies can use to deliver better services.
- Better information sharing is a democratic value, enabling transparency and open government.

Consequences of poor classification

There can be major consequences of incorrectly or not classifying government information.

- **No classification** – if information isn't classified users don't know how to protect or share it.
- **Under classification** – if information is under-classified there is a greater risk of it being compromised.
- **Over classification** – if information is over-classified it may be inaccessible to people with a need-to-know.

WHY IT MATTERS

KEY PRINCIPLES

- All information has value and requires an appropriate degree of protection.
- Access to classified information should only be granted based on a genuine ‘need to know’. Don’t over-classify, as this will ensure those who need it, have access to it.
- Information and assets received from, or exchanged with, external partners should be protected in accordance with any relevant legislative, regulatory, or international agreement requirements.
- Use sound online security practices. Stay abreast of best practice online behaviours when using mobile devices and working online.
- By applying good classification practices, you enable better information sharing, allowing agencies to make better decisions and deliver more effective services for New Zealanders.

Classification System

The Classification System provides a framework for assessing the potential harm generated to people, organisations, or government if the information were compromised. It defines the minimum requirements for secure handling of information to protect it.

The New Zealand Government has six security classifications broken into two categories that should be applied to all government information depending on the sensitivity of the information. All other information is considered unclassified.

There are a number of further protective markings (Endorsements) that can be applied to information to further restrict access to information.

Assessing harm

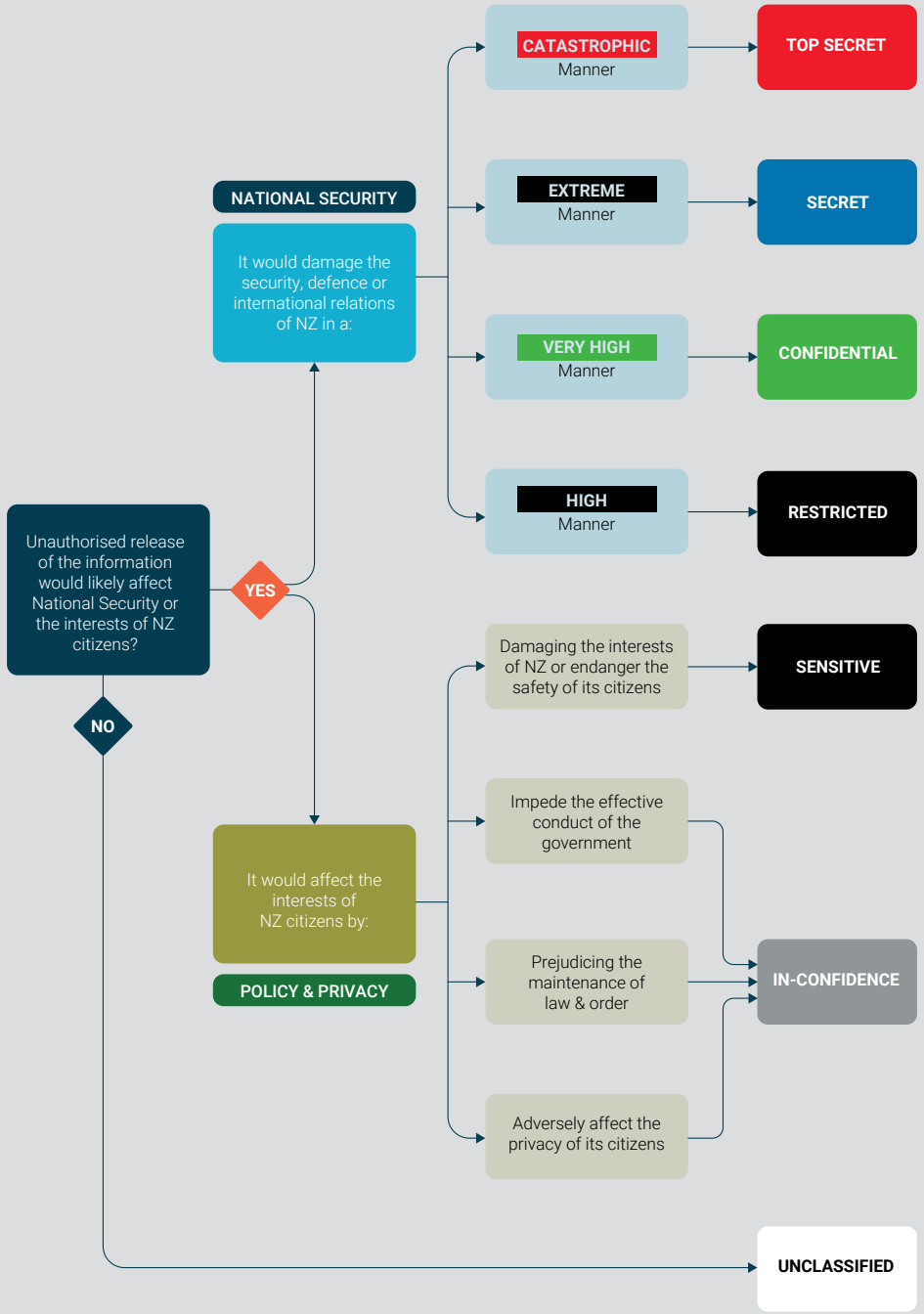
Government information is classified based on the harm compromise of that information may cause.

When you classify you are assessing the potential harm that compromise of the information will cause. This assessment will determine the classification level, and the security measures you need to apply to the information to reduce the likelihood of compromise.

To determine the harm that compromise of the information would cause, you need to determine the level of impact.

There are 6 impact levels:

IMPACT		HARM	CLASSIFICATION
1	**LOW**	Limited harm to people, organisations, or NZ national interest	**UNCLASSIFIED**
2	**MEDIUM**	Impede services, prejudice national interest, or breach personal privacy	**IN-CONFIDENCE**
3	**HIGH**	Damage national interest, disrupt services, or harm individuals	**SENSITIVE RESTRICTED**
4	**VERY HIGH**	Significant harm to defence, security, or international relations (short term)	**CONFIDENTIAL**
5	**EXTREME**	Extreme harm to defence, security, or international relations (medium term)	**SECRET**
6	**CATASTROPHIC**	Catastrophic harm to defence, security, or international relations (long term)	**TOP SECRET**



What are Protective Markings?

Protective markings are added to material to inform users of the sensitivity of the material and identify the special handling and security measures required to protect it from compromise.

Protective markings are separated into classifications and endorsements.

POLICY AND PRIVACY CLASSIFICATIONS

Information that is classified to protect national interest, national policy, or personal privacy. If compromised it could threaten the security or interests of people, organisations, government, or the community.

1 **IN-CONFIDENCE**

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

2 **SENSITIVE**

The compromise would likely cause harm to organisations, damage the interests of New Zealand, or endanger the safety or wellbeing of its citizens.

NATIONAL SECURITY CLASSIFICATIONS

Information that is classified to protect New Zealand's interests. If compromised it could threaten the security, defence, or international relations of the Government.

3 **RESTRICTED**

Compromise would likely adversely affect New Zealand's security, defence, or international relations.

4 **CONFIDENTIAL**

Compromise would likely cause significant (short term) damage to New Zealand's security, defence, or international relations.

5 **SECRET**

Compromise would likely cause extreme (medium term) damage to New Zealand's security, defence, or international relations.

6 **TOP SECRET**

Compromise would likely cause catastrophic (longer term) damage to New Zealand's security, defence, or international relations.

For further details please go to the PSR website:
www.protectivesecurity.govt.nz/classification-system

ENDORSEMENTS

lEndorsements warn people that information has special handling requirements. These are additional markings alongside the classification. These may include restricting access and dissemination based on need-to-know and special handling procedures. Agency specific policy and procedures will detail the endorsements used and any special requirements required for each endorsement.

Refer to PSR website for more information on endorsements.

Endorsement markings may indicate:

- the specific nature of information
- temporary sensitivities
- limitations on access and dissemination
- how recipients should handle or disclose information.

You should use endorsement markings only when there is a clear need for special care.

Remember that endorsement markings are not security classifications in their own right — they mustn't appear without a security classification.

How to protectively mark information

This section provides guidance on how to protectively mark information including documents, paragraphs, email, and verbal correspondence.

MARKING DOCUMENTS

Protective markings should be applied as follows:

Position: Centred top and bottom of each page
Case: CAPITAL LETTERS
Style: **BOLD**
Colour: Colour coded as per the following table to make them easily identifiable.
Size: Greater than 3mm in height (~12pt), or the same size at the body text (whichever is larger)

CLASSIFICATION	COLOUR	RGB	PARAGRAPH MARKING
UNCLASSIFIED	**BLACK**	(r0 g0 b0)	(U)
IN-CONFIDENCE	**BLACK**	(r0 g0 b0)	(IC)
SENSITIVE	**BLACK**	(r0 g0 b0)	(Sen)
RESTRICTED	**BLACK**	(r0 g0 b0)	(R)
CONFIDENTIAL	**GREEN**	(r0 g176 b80)	(C)
SECRET	**BLUE**	(r0 g0 b255)	(S)
TOP SECRET	**RED**	(r255 g0 b0)	(TS)

MARKING PARAGRAPHS

By protectively marking paragraphs you provide a clear mark of the sensitivity of the information throughout a document. This makes it easier to review, edit, share and declassify information.

Paragraph markings must:

- be the same font, weight, size and colour as the paragraph style
- be added at the beginning of each paragraph in brackets
- use the abbreviations shown in the previous table.
- not be applied to titles or headings.

The document marking must be classifed at the highest level of all the paragraph markings in the document.

MARKING EMAILS

Emails should be marked with appropriate protective marking.
The markings must appear as follows:

- In the subject line
- At the beginning of the email. Follow the classification colour coding as per document markings.

The classification must be:

- **BOLD**
- **ALL CAPS**

If you attach a classified document to your email, please ensure you mark the email at the same classification as the attached document, even if there is no classified information within the actual email text.

SECURE AND ENCRYPTED EMAIL (SEEMAIL)

SEEMail is the New Zealand Government's accredited secure and encrypted email service. It secures email sent over the internet between participating New Zealand Government public sector organisations and trusted partners.

- **SENSITIVE** or **RESTRICTED** information cannot be sent via email unless it will remain within an end-to-end accredited encrypted system such as SEEMail.
- **IN-CONFIDENCE** emails do not need to be encrypted but is good practice to do so if the receiving organisation is a participating SEEMail user.
- **CONFIDENTIAL, SECRET** or **TOP SECRET** information cannot be emailed using SEEMail, this information requires an accredited GCSB system.

Tagging emails

SEEMail uses specific 'trigger words' to apply appropriate protective measures to emails. Add square brackets around the classification and use the appropriate tags depending on who you want to receive the email:

TRIGGER WORDS	WHO CAN RECEIVE
[SEEMAIL]	Limits sending to only participating SEEMail government agencies. Use this trigger word for securely sending unclassified communication.
[TRUSTED]	Allows sending to both SEEMail participating government agencies and trusted partners. Use this trigger word for securely sending unclassified communication.
[RESTRICTED]	Limits sending to agencies or partners accredited to RESTRICTED SEEMail systems.
[SENSITIVE]	Limits sending to agencies or partners accredited to RESTRICTED SEEMail systems.
[IN-CONFIDENCE]	Allows sending to any participating SEEMail user.

Handling classified information

Handling of classified information may be controlled due to its sensitivity. Access to any classified information will be based on a clear need-to-know requirement further restricting access.

Secure all classified material on your desk when leaving your workspace unattended.

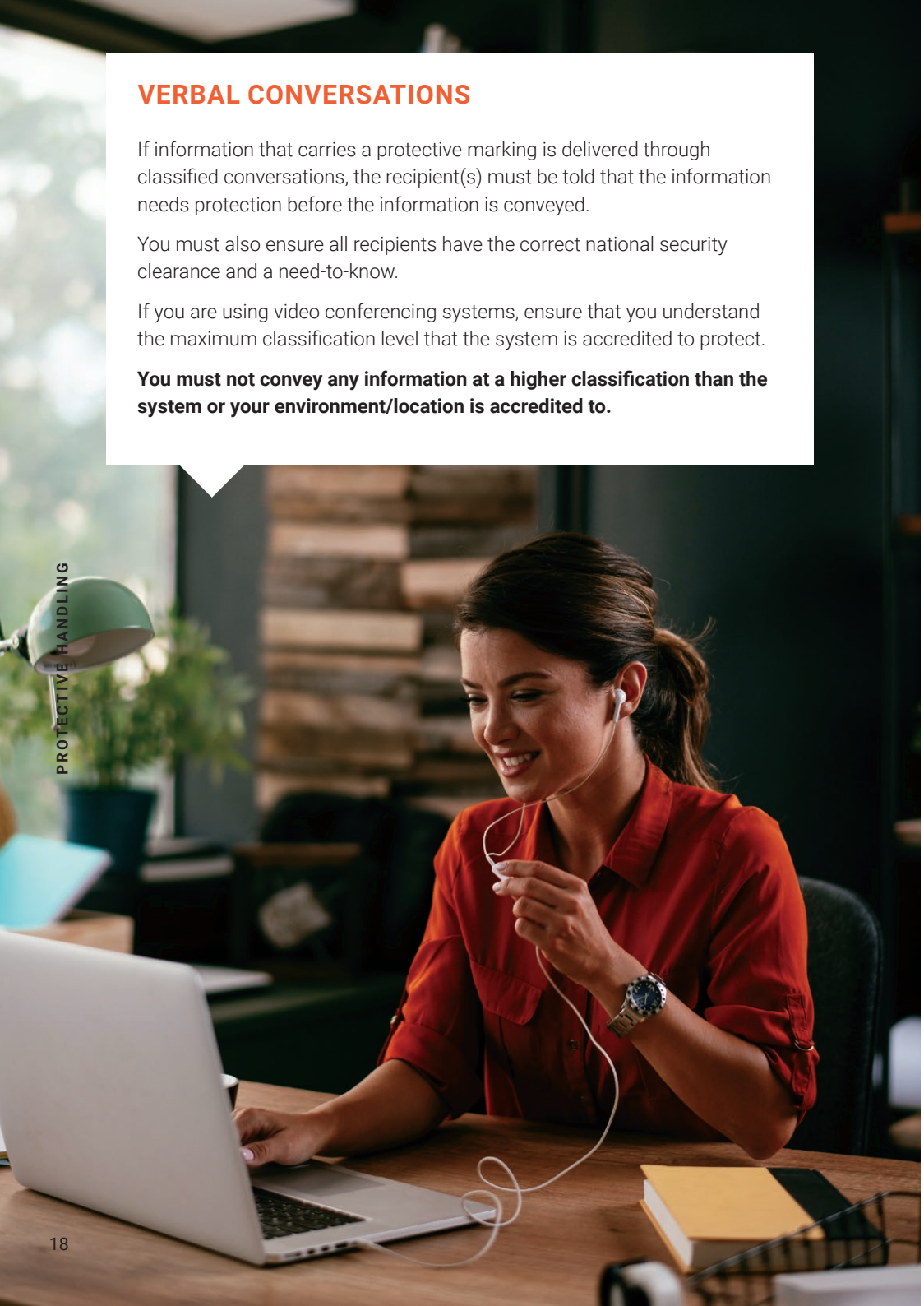
Lock your computer screen when walking away from your computer, or someone approaches your workspace.

You must obtain originator agreement prior to printing, copying, sharing, or removing classified information. Copies should not be left unattended on printers.

Check your surroundings. Conversations and meetings discussing classified information must be held only in the appropriate secured area to prevent being overheard and compromise of the information.

Do not share information at higher classifications than the ICT system is certified to process including telephones and networks. Refer to your security team for more information.

Refer to the Classification Quick Guides on the PSR website and follow your agency's policies and procedures.



VERBAL CONVERSATIONS

If information that carries a protective marking is delivered through classified conversations, the recipient(s) must be told that the information needs protection before the information is conveyed.

You must also ensure all recipients have the correct national security clearance and a need-to-know.

If you are using video conferencing systems, ensure that you understand the maximum classification level that the system is accredited to protect.

You must not convey any information at a higher classification than the system or your environment/location is accredited to.

Transporting classified information

The security measures required to protect information during physical transfer depend on:

- the level of protective markings
- the origin and destination
- the method used for transport.

The intended recipient must have the appropriate 'need-to-know' and the required level of security clearance before the information is transferred.

You must use security measures to protect marked information when it is in transit. Please refer to the Classification Quick Guides on the PSR website and follow your agency's policies and procedures.

Receiving classified material

Before you allow anyone in your agency to receive hard copies of protectively-marked information, make sure they are aware of their responsibilities and, when necessary, hold the appropriate security clearance.

Protectively-marked documents should only be opened by the intended recipient or the alternative recipient. However, your agency head may authorise a specified person or area to open all mail and perform the related information or security management functions.

When someone other than the intended recipient is charged with its opening, adopt the normal practice of opening the outer envelope only. The inner envelope should only be opened in the presence of the intended recipient.

Destroying classified information

Destruction of classified information and assets must be done in accordance with the Public Records Act 2005, PSR, and NZISM. Refer to your agency's destruction policy and procedures.

When approved to be destroyed:

- Keep classified waste separate from unclassified waste and secured until destroyed. Classified waste bags or bins must be protected under same requirements for the highest classification level.
- You must not use standard rubbish or recycling services to dispose of classified material unless already destroyed appropriately (e.g. shredded)
- Use approved procedures for secure destruction of ICT media or equipment.

Consideration for remote working

Remote working is now the norm, yet many people are unaware of the threats that they face.

You may take work home, work in the field, work from hotels or conference venues, visit client offices, or work while on public transport. Remote working increases the risk of compromise and may result in loss or theft of sensitive and high-value government information.

Your obligations are to:

- before removing or transporting classified information from the workplace, obtain approval from your manager (and originator if applicable)
- prevent overlooking and overhearing while in transit and at unsecure locations
- store classified information under lock and key
- encrypt removable media and devices
- follow your agency's policies and procedures for remote working.

Refer to the PSR mobile and remote working guidance for more information.

Your classification responsibilities

- ☑ You have a legal obligation to protect all information to enable its safe use, handling, and sharing.
- ☑ You must classify information based on the assessment of harm that compromise of the information would cause.
- ☑ Think about your audience when creating information so that its classification doesn't become a barrier to its use.
- ☑ By applying good classification practices, you enable better information sharing, allowing agencies to make better decisions and deliver more effective services for New Zealanders.
- ☑ Regularly review information's sensitivity, as its classification may have changed in response to specific conditions, events or time lapse.

For more information regarding your legal obligations please refer to the following main pieces of legislation supporting the classification system that govern how you collect, disclose and use of government information.

- Offical Information Act 1982
- Privacy Act 2020
- Public Records Act 2005.

Practical Tips

Use paragraph markings to make it easier to identify what information is appropriate for different audiences.

When creating information, consider how it can be proactively released to the public.

If you are not sure why information has specific protective markings, ask its creator. You must never change someone else's protective marking without asking them first.

Review protective markings to ensure they are still appropriate when creating, editing, using, or sharing information.

Talk to your colleagues and security advisors if you are unsure about the correct protective markings.

For more information, go to:

www.protectivesecurity.govt.nz

psr@protectivesecurity.govt.nz

Te Kāwanatanga o Aotearoa
New Zealand Government

VERSION 1 / JUNE 2022

PSR | Protective Security Requirements