Information classification and protection

Table of Contents

Information classifications

Security classifications specify how people must protect the information and equipment they handle. Police use the NZ government classifications as defined on the PSR Classification System webpages.

IN CONFIDENCE classification

IN CONFIDENCE information is that in respect of which: "compromise would prejudice the maintenance of law and order, impede organisation operations, or affect adversely the privacy of its citizens".

IN CONFIDENCE includes information where compromise might:

- impede non-critical services or inconvenience an organisation but not prevent them from delivering services
- prejudice the preservation of law and order or New Zealand's economic interests such as prejudicing Police or Justice investigations or prosecutions
- breach obligations of confidence such as legal or professional privilege
- prejudice an organisation's negotiation with a supplier
- breach a person's privacy but does not endanger their safety or wellbeing

Most Police information relating to law enforcement is INCONFIDENCE. For example, at Police, this includes:

- Information about any person
- Files relating to incidents, investigations, prosecutions, complaints, or internal disciplinary matters.
- Operational orders which disclose intended tactics.
- Tenders, proposals, or contracts with prices or proprietary information.
- Legal advice on official Police matters.

See the Information Protection section for the minimum requirements to protect IN CONFIDENCE information, but in summary, it:

- must be stored in an area that is not accessible by visitors or the public;
- may be prepared and held on the Police Enterprise system and other authorised systems;
- should be clearly marked IN CONFIDENCE in any electronic transmission; and
- must only be disposed of (in hard copy) by shredding or secure waste or (in electronic form) by file or device sanitisation (i.e. overwriting) or destruction.

SENSITIVE classification

SENSITIVE information as that in respect of which: "Compromise would cause harm to organisations, damage the interests of New Zealand or endanger the safety or wellbeing of its citizens." SENSITIVE includes information where compromise might:

- endanger the safety of any person or materially harm their wellbeing or livelihood
- disrupt organisational services
- cause loss of trust with the public
- disadvantage government negotiations
- prematurely disclose information on government policies that has economic or financial consequences
- harm our ability to prevent, detect, or investigate offences
- affect the security or resilience of national infrastructure or services

Examples of SENSITIVE information held by Police are victim statements containing highly personal information, medical records and witness protection information.

It differs from other classifications in that although the minimum protective standard for it is the same as for RESTRICTED, there may be varying degrees of sensitivity, so the level of security required may also need to vary. Consideration should be given to the use of endorsements to signify the need to further limit its circulation.

See the Information Protection section for the minimum requirements to protect SENSITIVE information, but in summary, it:

- must be stored in a locked drawer, cabinet or similar, even within Police premises;
- may be prepared and held on Police systems;
- may only be sent by email to Government agencies by SEEMail or another approved system; and
- must only be disposed of (hard copy) by shredding, or (in electronic form) by device destruction and, in some cases, device sanitisation (i.e. overwriting).

RESTRICTED classification

RESTRICTED information is that in respect of which: "Compromise would adversely affect New Zealand's national interest, security, defence or international relations." RESTRICTED includes information where compromise might:

- degrade the effectiveness of agencies working in national security areas
- degrade defence or security operational effectiveness such that operations may need to be replanned, reprioritised, or delayed
- adversely affect New Zealand’s diplomatic relations such as affect negotiations with a nation
- adversely affect economic, scientific, or technological matter vital to New Zealand’s stability or integrity

For example, at Police, this includes:

- Some Protection Services information about foreign representatives or foreign mission premises.
- Intelligence, investigations or operations with possible links to terrorism or trans-national crime.
- Any Police information that references RESTRICTED information originating from another agency.
- Material prepared for interagency exercises related to national security.

This classification should be used sparingly. Consideration should be given to the use of endorsements to signify the need to further limit circulation of material.

The minimum protection requirements for RESTRICTED are the same as for SENSITIVE.

There are three national security classifications higher than RESTRICTED. They are CONFIDENTIAL, SECRET, TOP SECRET, and are described in Working with information classified CONFIDENTIAL and above. Police are recipients of such information and intelligence, and may be involved in joint operations that are related to national security matters. However, Police-generated information will rarely reach this threshold.

Endorsement markings

Endorsement markings may be used in conjunction with any of the classifications when there is a need for special care, in order to indicate the specific nature of the information, temporary sensitivities, or limitations on availability, circulation or access.

This table shows the types of endorsements used for security classification purposes.

Type	When the endorsement is commonly used
<Addressees> only	Material that must be seen only by the people to whom it is addressed. A group or tier could be substituted e.g., "SENSITIVE EXECUTIVE ONLY".
Appointments	Actual or potential appointments that have not been announced and records of the deliberation during the recommendation/approval process.
Budget	Proposed or actual measures for the Budget prior to their announcement by the Government.
Cabinet	Contains material which will be presented to, and/or require decisions by, Cabinet or Cabinet Committee.
Commercial	Information about guarded commercial processes; or about negotiations or business affairs where disclosure may adversely affect a commercial position.
Embargoed for release	The information is to be protected only until the time or date designated in the body of the document at which time it may be released or disseminated.
Evaluative	Material relating to comparative evaluations of people, such as employment candidate assessments or interview records; or of products or services through tender assessments.
Exercise	Material written or adapted for input to exercises where premature disclosure to participants would lessen its educative value.
Honours	The actual or potential award of an honour before the announcement of Royal prerogative awards, and the deliberations during the recommendation/approval process.
Legal Privilege	This marking may be used for material that is subject to legal privilege.
Medical	Medical reports, records and other material relating to them.
NZ eyes only (NZEO)	Material not to be viewed by any person who is not a New Zealand national.
Police use only	For use only within NZ Police.
Policy	Proposals for new or changed Government policy before publication.
Releasable to (REL)	Identifies information that has been released or is releasable to the indicated foreign countries or citizens of those indicated countries only. For example, REL // NZ, CAN.
Staff	References to named or identifiable staff -especially if private matters are involved. May also be used by staff for entrusting personal confidences to management.
To be reviewed on <date>	A designated time at which the classification of the information is on to be reviewed.

Applying security classifications

Where possible, originators should assess and apply the correct classification before information is stored, processed or communicated. The consequence of classified information having been handled by a system that is not authorised for that level of classification can be significant and costly. Conversely, over-classifying can result in expensive or inconvenient protection being used unnecessarily.

All classified information should be marked with its classification, including IN CONFIDENCE if it could help others to manage it appropriately. The marking should be done as soon as the information is assessed (usually when it is created). If the contents of a file, folder, binder or box comprise material of different classifications, the highest classification (only) must marked be on the cover.

Print or stamp the classification and the endorsement, if any, in BOLD UPPERCASE black lettering on both top and bottom centre of each page of a document. The text should be the same size as the body copy or at least 3mm in height (12pt), whichever is larger.

Classified documents should include page numbering, with total number of pages identified. Documents classified RESTRICTED and above should also use copy numbering for hard copies

If SENSITIVE or RESTRICTED information is conveyed orally, the recipients should also be advised of its classification.

Aggregated information

Some collections of information could justify a higher classification or additional security controls than the individual documents or pieces of information, due the increased business impact from the compromise of confidentiality, loss of integrity or unavailability of the combined collection. Such collections are normally referred to as ‘aggregated information’ or ‘aggregations’ and could include databases, discrete data collections relating to specific projects or operations, data stored in information systems or collections of hardcopy records.

Information protection

This section contains the minimum standards for the protection of IN CONFIDENCE, SENSITIVE and RESTRICTED classified information.

6(a) OIA

Requests for the non-compliance with minimum standards of security for classified material

In exceptional circumstances (e.g., threat to life), you may need to consider releasing information that would otherwise be prohibited. In those cases, the information must not be released without prior authorisation from a member of the Police Executive or Director: Capability. Any such request must include details relating to the operational imperative. The request and approval should be in writing and must be reported via the Security and Privacy Incident Register. If the information is owned by another agency, then that agency must also be advised as soon as practicable.

Use of document protection

Document protection, such as Microsoft Office or Peazip password protection, may be used if it is justified by an assessment. It offers a limited degree of privacy for short-term uses such as:

- unclassified or IN CONFIDENCE Police information temporarily held on a non-Police computer
- transmissions of IN CONFIDENCE information over public networks
- limited-circulation documents held on a shared drive
- for an additional layer of protection for SENSITIVE or RESTRICTED information within the Police environment.

However, unnecessary document protection can make it difficult to manage and use official records, so it should be used with care. Consider providing contingency access to your manager or team member, and removing the document protection when it is no longer needed.

Refer to the Head IT Security Management for approved document protection methods and products.