Classification Quick Guide

IN-CONFIDENCE

Control and handling requirements

Applying markings

Document markings

Case:	CAPITAL LETTERS
Style:	**BOLD**
Colour:	**BLACK** *(r0 g0 b0)*
Size:	Greater than 3mm in height (~12pt), or the same as body copy (whichever is larger)
Position:	Centred top and bottom of each page

Paragraph marking

Use paragraph markers when documents contain information at different classification levels. For paragraphs at IN-CONFIDENCE, use:

Paragraph marker: (IC)

(IC) paragraph marking appears at the start of each paragraph in brackets using the same font, weight and style as the paragraph. Paragraph markings should not be applied to titles or headings.

Personnel access

If a person needs access to government information, assets, or work locations marked IN-CONFIDENCE for their role, they do not need a national security clearance.

Government information and equipment are for official use for all who need it.

An endorsement to IN-CONFIDENCE information may limit access to and apply special handling requirements to the information in accordance with agency's policies and procedures.

Store and file

Keep government information at IN-CONFIDENCE secure through physical security measures aimed to keep unauthorised people out of areas where classified information is handled.

Physical materials and equipment at IN-CONFIDENCE should generally be stored in Security Zone 2 (Work area) or higher. However, if appropriately secured and accessed controlled, IN-CONFIDENCE information and equipment can also be stored in Security Zone 1 (Public Access area).

Physical files for IN-CONFIDENCE material are uncoloured.

Electronic information at IN-CONFIDENCE should be protected against illicit internal use or external intrusion through two or more mechanisms:

- User challenge and authentication (requiring username and password, digital ID, or digital certificate)
- Logging use at level of individual
- Firewalls and intrusion detection systems and procedures
- Server authentication
- Security measures specific to the operating system or application you use.

Classification Quick Guide

IN-CONFIDENCE

Control and handling requirements

Use, copy or share

Your agency should consider implementing a clear desk and screen policy to protect IN-CONFIDENCE information against accidental or opportunistic compromise during its use.

You must obtain originator agreement prior to printing, copying or sharing IN-CONFIDENCE information.

Only reproduce information when necessary and keep the number of copies to a minimum. All reproduced information must retain the original markings or higher.

When required to control the number of copies, ask the originator to supply any additional copies needed.

Consider the sensitivity of the information and if appropriate, use encryption when emailing or transmitting IN-CONFIDENCE information (e.g., use SEEMail if possible). Consider use of access controls when transmitting or sending.

You must not use or share information at higher classifications than the ICT system is accredited to protect. For example, many common cloud applications are not accredited to share classified information. Refer to your security team to understand the accreditation level of the ICT systems you use.

When communicating government information via email, include a communication of the recipient's legal and destruction obligations if the incorrect party receives it. .

Remove or transport

Removal of IN-CONFIDENCE information or equipment from your premises should be authorised by the originator or controlling organisation and in accordance with agency policy.

Removable media usage is governed by the agency's policy.

You must use security measures to protect marked information when it is in transit.

When transporting between locations, IN-CONFIDENCE information may be carried by post, courier service, or your mail delivery staff. Use your security risk management plan to inform decisions as to whether transporting IN-CONFIDENCE information requires double enveloping.

The envelope must clearly show a return address if undeliverable. To protect the organisation's privacy, you can use a return PO Box.

Never mark classifications or protective markings on envelopes.

Archive or disposal

Archival and disposal of public records must be done in accordance with the Public Records Act 2005. Refer to your organisation's information and records management policies and procedures.

Archive or dispose of IN-CONFIDENCE information or equipment by agency arrangements and procedures.

When you dispose of electronic government information, ensure the waste can't be reconstructed or used.

Control and handling requirements

SENSITIVE | **RESTRICTED**

Applying markings

Document markings

Case: CAPITAL LETTERS

Style: **BOLD**

Colour: **BLACK** *(r0 g0 b0)*

Size: Greater than 3mm in height (~12pt), or the same as body copy (whichever is larger)

Position: Centred top and bottom of each page

Numbering: Page numbering is essential, with total number of pages identified. Copy number is essential.

Paragraph marking – SENSITIVE

Use paragraph markers when documents contain information at different classification levels. For paragraphs at SENSITIVE, use:

Paragraph marker: (Sen)

(Sen) paragraph marking appears at the start of each paragraph in brackets using the same font, weight and style as the paragraph. Paragraph markings should not be applied to titles or headings.

Paragraph marking – RESTRICTED

For paragraphs at RESTRICTED, use:

Paragraph marker: (R)

(R) paragraph marking appears at the start of each paragraph in
brackets using the same font, weight and style as the paragraph.
Paragraph markings should not be applied to titles or headings.

Personnel access

A person does not need a national security clearance, but agencies may undertake their own security clearance process before granting access. (e.g MoJ or Police checks). See the agency's policies and procedures to confirm.

An endorsement to SENSITIVE and RESTRICTED information may further limit access and apply special handling requirements to the information in accordance with agency's policies and procedures.

Archive or disposal

Archive and disposal of public records must be done in accordance with the Public Records Act 2005.

Waste of SENSITIVE and RESTRICTED information and equipment must be kept separate from unclassified waste and secured under same precautions as Store and File.

Must not be disposed by standard rubbish or recycling collection unless it has already been through an approved destruction process (e.g. shredding).

Originator may require shared information to be returned for archival or disposal.

Only appropriate NZSIS-approved equipment systems must be used for destruction of paper waste. See Destruction methods for more information.

ICT media and equipment must undergo sanitisation or destruction in accordance with the NZISM 13. Media and IT Equipment Management, Decommissioning and Disposal.

When you dispose of electronic government information, ensure the waste can't be reconstructed or used.

Store and file

Keep government information at SENSITIVE and RESTRICTED information or equipment physically stored in Zone 2 in a lockable storage area or cabinet when not in use. When in use, material or equipment should not be left unattended or unsecured.

In a storage facility, SENSITIVE and RESTRICTED information and equipment should be protected through controlled access to the storage areas, and through a secure physical environment.

Physical files for SENSITIVE and RESTRICTED material are uncoloured or black.

Electronic information (including databases) at SENSITIVE and RESTRICTED should be protected against illicit internal use or external intrusion through two or more mechanisms:

- User challenge and authentication (requiring username and password, digital ID, or digital certificate)
- Logging use at level of individual
- Firewalls and intrusion detection systems and procedures
- Server authentication
- Security measures specific to the operating system or application you use.

ICT media or equipment holding SENSITIVE or RESTRICTED information must be encrypted and stored in compliance with NZISM 13 Media and IT Equipment Management, Decommissioning and Disposal.

Control and handling requirements

SENSITIVE | **RESTRICTED**

Use, copy or share

Information at SENSITIVE and RESTRICTED, can be used in Zone 1 (Public Areas) but storage is not recommended but permitted if unavoidable (see Store and File requirements.)

Encryption is mandatory for emailing or transmitting SENSITIVE and RESTRICTED information across public networks within New Zealand or across any networks overseas using a system approved by GCSB (e.g. use of SEEMail or other international accredited systems).

You must obtain originator agreement prior to printing, copying or sharing SENSITIVE and RESTRICTED information. Printing, copying, reproducing or sharing may be prohibited by the originator or controlling agency or government. Copies should not be left unattended on printers or devices.

All reproduced information must retain the original markings or higher.

Face-to-face or virtual conversations and meetings discussing or sharing SENSITIVE and RESTRICTED information must be held only in secured areas and using only accredited ICT systems and networks the same classification level to prevent information compromise.

ICT media or equipment holding SENSITIVE and RESTRICTED information must be handled and used in compliance with NZISM 13 Media and IT Equipment Management, Decommissioning and Disposal.

Remove or transport

Removal of SENSITIVE and RESTRICTED information or equipment from your premises should be authorised by the originator or controlling organisation and in accordance with agency policy and basis of real need. For example, when going to a meeting.

You must use security measures to protect marked information when it is in transit.

For removal or transport for mobile or remote work, refer to the PSR's Mobile and remote working for more information.

SENSITIVE and RESTRICTED information or equipment may be carried by safe hand, postal service, or commercial courier service for domestic transport and via diplomatic airfreight via MFAT internationally. Never mark classifications or protective markings on external envelopes.

Use your security risk management plan to inform decisions as to whether transporting SENSITIVE and RESTRICTED information requires double enveloping.

When moving SENSITIVE and RESTRICTED information or equipment by safe hand:

Within a single location:

It may be passed uncovered, by hand, provided it always in personal custody of an authorised person and there is no opportunity for it to be compromised.

Between locations within New Zealand:

Use a single closed, opaque envelope and delivered direct, by hand, to the recipient by an authorised messenger. Use of receipts is at the discretion of the originator.

The envelope is enclosed in a NZSIS approved briefcase, satchel, or pouch to move between locations.

When transporting by post, commercial courier, or MFAT diplomatic airfreight service:

It must be double enveloped and evidence of receipt is required (e.g. track and trace).

Address the envelope to the individual by name and title. Return address clearly shown if undeliverable. Use a PO Box if required.

If sent overseas, all of the above plus carried by diplomatic airfreight via the Ministry of Foreign Affairs and Trade (MFAT). See MFAT for more information

Control and handling requirements

CONFIDENTIAL

Applying markings

Document markings

Case: CAPITAL LETTERS

Style: **BOLD**

Colour: **GREEN** *(r0 g176 b80)*

Size: Greater than 3mm in height (~12pt), or the same as body copy (whichever is larger)

Position: Centred top and bottom of each page

Paragraph marking

Use paragraph markers when documents contain information at different classification levels. For paragraphs at CONFIDENTIAL, use:

Paragraph marker: (C)

(C) paragraph marking appears at the start of each paragraph in
brackets using the same font, weight and style as the paragraph.
Paragraph markings should not be applied to titles or headings.

Personnel access

A person needs a national security clearance of CONFIDENTIAL or higher level to obtain access to CONFIDENTIAL information. This includes all people involved with transmission, storage and disposal of CONFIDENTIAL information or equipment.

Information classified at CONFIDENTIAL must be held, processed, transmitted and destroyed with levels of security commensurate with the significant damage to national security that compromise would incur.

Information and equipment at CONFIDENTIAL require consideration for controlling access and special handling requirements based on the protective markings in accordance with agency's policies and procedures.

Store and file

Keep government information at CONFIDENTIAL physically stored in Security Zone 3 (Restricted Work Area) or higher but can be stored in Zone 2 (Work Area) if adequately protected from unauthorised access.

Information and equipment at CONFIDENTIAL must be locked in an approved security container when not in use. The minimum acceptable storage arrangements are a combination of (see Security containers and cabinets for more information):

- The protection afforded by the security container itself
- The position or site (Security Zone)
- The use of approved security equipment.

It is good security practice to keep a record of incoming and outgoing CONFIDENTIAL information in a Classified Document Register.

Printed material is immediately placed in a folder to prevent unauthorised access. Physical file folders for CONFIDENTIAL material are green.

Electronic information is protected against illicit use or intrusion using two or more following mechanisms:

- Username / password or digital ID/Certificate
- Logging use at level of individual
- Firewalls and intrusion detection systems and procedures
- Server authentication
- Security measures specific to the operating system or application you use.

ICT media and systems holding CONFIDENTIAL information must be in compliance with the NZISM.

Control and handling requirements

CONFIDENTIAL

Use, copy or share

Information at CONFIDENTIAL, can be used in Zone 1 (Public Areas) but storage is not recommended but permitted if unavoidable (see Store and File requirements.)

Clear desk policy is mandatory.

Emailing or transmitting of CONFIDENTIAL information is not allowed across public networks and can only be transmitted using a system approved and accredited by the GCSB.

You must obtain originator agreement prior to printing, copying or sharing CONFIDENTIAL information. Printing, copying, reproducing or sharing may be prohibited by the originator or controlling agency or government. All reproduced information must retain the original markings or higher.

Copies should not be left unattended on printers or devices.

Conversations and meetings discussing CONFIDENTIAL information must be held only in appropriate zone secured areas to prevent information compromise.

ICT media or equipment holding CONFIDENTIAL information must be handled and used in compliance with NZISM 13 Media and IT Equipment Management, Decommissioning and Disposal.

Remove or transport

Removal of CONFIDENTIAL information or equipment from your premises should be authorised by the originator or controlling organisation and in accordance with agency policy and basis of real need. For example, when going to a meeting.

You must use security measures to protect marked information when it is in transit.

CONFIDENTIAL information or equipment must be in personal custody of authorised individuals and kept in NZSIS approved container when being transported.

Moving CONFIDENTIAL information or equipment within a single location

Use a single closed, opaque envelope indicating the classification. Use of receipts is at the discretion of the originator. And either:

- Passed by hand between people who have the appropriate security clearance and 'need to know', or
- Placed in a NZSIS-approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger.

It may be passed uncovered, by hand, within a discrete office environment provided it always in personal custody of an authorised person with the appropriate security clearance and 'need to know' and there is no opportunity for it to be compromised.

Moving CONFIDENTIAL information between locations within New Zealand Deliver by safe hand:

- Double enveloping is required AND receipting is required AND one of the following:
- Placed in an NZSIS-approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger
- Delivered by NZSIS-approved courier
- Delivered by an agency specific alternative approved by NZSIS.

Or deliver by commercial courier if no safe hand service is available.

- Double enveloping is required AND receipting is required AND delivered by commercial courier AND both agencies agree.

Moving CONFIDENTIAL information outside of New Zealand Deliver by safe hand:

- Double enveloping is required AND receipting is required AND one of the following:
- Delivered by MFAT courier service- See MFAT for more information.

Archive or disposal

Archive and disposal of public records must be done in accordance with the Public Records Act 2005.

Waste of CONFIDENTIAL information and equipment must be kept separate from unclassified or RESTRICTED waste and secured under same precautions as Store and File.

Must not be disposed by standard rubbish or recycling collection unless it has already been through an approved destruction process (e.g. shredding.)

Originator may require shared information to be returned for archival or disposal.

Only appropriate NZSIS-approved equipment must be used for destruction of paper waste. See Destruction methods for more information.

If ACCOUNTABLE MATERIAL, destruction of paper waste must be done under supervision of two authorised officers who must supervise the removal of the material to the point of destruction, ensure destruction is complete, and sign a destruction certificate.

ICT media and equipment must undergo sanitisation or destruction in accordance with the NZISM 13. Media and IT Equipment Management, Decommissioning and Disposal.

When you dispose of electronic government information, ensure the waste can't be reconstructed or used.

Control and handling requirements

SECRET

Applying markings

Document markings

Case: CAPITAL LETTERS

Style: **BOLD**

Colour: **BLUE** *(r0 g0 b255)*

Size: Greater than 3mm in height (~12pt), or the same as body copy (whichever is larger)

Position: Centred top and bottom of each page

Numbering: Page numbering is essential, with total number of pages identified. Include serial number if in series.

Paragraph marking

Use paragraph markers when documents contain information at different classification levels. For paragraphs at SECRET, use:

Paragraph marker: (S)

(S) paragraph marking appears at the start of each paragraph in brackets using the same font, weight and style as the paragraph. Paragraph markings should not be applied to titles or headings.

Personnel access

A person needs a national security clearance of SECRET or higher level to obtain access to SECRET information.

Information classified at SECRET must be held, processed, transmitted and destroyed with levels of security commensurate with the serious damage to national security that compromise would incur.

Information and equipment at SECRET require consideration for controlling access and special handling requirements based on the protective markings in accordance with agency's policies and procedures.

Store and file

Keep government information at SECRET physically stored in Security Zone 4 (Security Areas) or higher but can be stored in Security Zone 3 (Restricted Work Area) if adequately protected from unauthorised access and stored within an approved security container.

Information and equipment at SECRET must be locked in an approved security container when not in use. The minimum acceptable storage arrangements are a combination of (see Security containers and cabinets for more information):

- The protection afforded by the security container
- The position or site (Security Zone)
- The use of approved security equipment.

It is good security practice to keep a record of incoming and outgoing SECRET information in a Classified Document Register.

Printed material is immediately placed in a folder to prevent unauthorised access. Physical file folders for SECRET material are blue.

If declared as ACCOUNTABLE MATERIAL, it must be recorded in Classified Document Register with a reference number and copy number.

Electronic information is protected against illicit use or intrusion using two or more following mechanisms:

- Username / password or digital ID/Certificate
- Logging use at level of individual
- Firewalls and intrusion detection systems and procedures
- Server authentication
- Security measures specific to the operating system or application you use.

ICT media and systems holding SECRET information must be in compliance with the NZISM.

Control and handling requirements

SECRET

Use, copy or share

Information at SECRET, can be used in Zone 2 (Public Areas) but storage is not permitted.

Clear desk policy is mandatory.

Emailing or transmitting of SECRET information is not allowed across public networks and can only be transmitted using a system approved and accredited by the GCSB.

You must obtain originator agreement prior to printing, copying or sharing SECRET information. Printing, copying, reproducing or sharing may be prohibited by the originator or controlling agency or government. Copies should not be left unattended on printers or devices.

Conversations and meetings discussing SECRET information must be held only in appropriate zone secured areas to prevent information compromise.

ICT media or equipment holding SECRET information must be handled and used in compliance with NZISM 13 Media and IT Equipment Management, Decommissioning and Disposal.

Remove or transport

Removal of SECRET information or equipment from your premises should be authorised by the originator or controlling organisation and in accordance with agency policy and basis of real need. For example, when going to a meeting.

You must use security measures to protect marked information when it is in transit.

SECRET information or equipment must be in personal custody of authorised individuals and kept in NZSIS approved container when being transported.

When moving SECRET information or equipment within a single location

Double envelope and use of an approved seal.

You have three options for manually transporting SECRET information:

- Dispatch through your transit system with hand-to-hand receipts at each stage of the journey.
- Distribute within a building or part of a building that has been declared a specially-protected area – a Secure Compartmented Information Facility (SCIF). May be passed uncovered, provided it is transported directly between people with appropriate clearance and 'need-to-know' and there is no opportunity for any unauthorised person to view the information.
- Carried via an authorised, security-vetted messenger in an NZSIS-approved briefcase, satchel, or pouch and transported directly to the authorised recipient.

When moving SECRET information between locations within New Zealand

SECRET material must be:

- Double enveloped
- Sealed with an approved seal
- Carried via an authorised, security-vetted messenger or safe hand courier.

When moving SECRET information outside of New Zealand

SECRET material must be:

- Double enveloped with a receipt from inside the inner envelope
- Sealed with an approved seal
- Carried via MFAT Diplomatic Safe Hand Courier Service – See MFAT for more information.

Archive or disposal

Archive and disposal of public records must be done in accordance with the Public Records Act 2005. Unless required for archival purposes, SECRET material should be destroyed as soon as possible once it is no longer required for operational purposes.

Originator may require shared information to be returned for archival or disposal.

Only appropriate NZSIS-approved equipment systems must be used for destruction of paper waste. See Destruction methods for more information.

If ACCOUNTABLE MATERIAL, destruction of paper waste must be done under supervision of two authorised officers who must supervise the removal of the material to the point of destruction, ensure destruction is complete, and sign a destruction certificate. If you need to account for SECRET information you destroy, record its destruction in your Classified Document Register.

ICT media and equipment that has held SECRET information must be declassified by degaussing, overwriting, or destroying in accordance with the NZISM 13. Media and IT Equipment

Control and handling requirements

TOP SECRET

Applying markings

Document markings

Case: CAPITAL LETTERS

Style: **BOLD**

Colour: **RED** *(r255 g0 b0)*

Size: Greater than 3mm in height (~12pt), or the same as body copy (whichever is larger)

Position: Centred top and bottom of each page

Numbering: Page numbering is essential, with total number of pages identified. Copy number is essential.

Paragraph marking

Use paragraph markers when documents contain information at different classification levels. For paragraphs at TOP SECRET, use:

Paragraph marker: (TS)

(TS) paragraph marking appears at the start of each paragraph in brackets using the same font, weight and style as the paragraph.

Paragraph markings should not be applied to titles or headings.

Personnel access

A person needs a national security clearance of TOP SECRET or TOP SECRET SPECIAL to obtain access to TOP SECRET information.

Information classified at TOP SECRET must be held, processed, transmitted and destroyed with levels of security commensurate with the catastrophic damage to national security that compromise would incur.

Information and equipment at TOP SECRET require consideration for controlling access and special handling requirements based on the protective markings in accordance with agency's policies and procedures.

Archive or disposal

Archive and disposal of public records must be done in accordance with the Public Records Act 2005. Unless required for archival purposes, TOP SECRET material should be destroyed as soon as possible once it is no longer required for operational purposes.

Before destroying TOP SECRET information manually, verify that all pages and enclosures are present (nothing is missing):

The destruction must be supervised and witnessed by two authorised officers who must supervise the removal of the material to the point of destruction, ensure destruction is complete, and sign a destruction certificate.

Only appropriate NZSIS-approved equipment systems must be used for destruction of TOP SECRET. See Destruction methods for more information.

Record the destruction within the Classified Document Register.

ICT media and equipment that has held TOP SECRET information cannot be declassified. It must be destroyed in accordance with the NZISM 13. Media and IT Equipment Management, Decommissioning and Disposal.

Store and file

Keep government information at TOP SECRET physically stored in Security Zone 5 (High-Security Areas) or SCIF.

Information and equipment at TOP SECRET must be locked in an approved security container when not in use. The minimum acceptable storage arrangements are a combination of (see Security containers and cabinets for more information):

- The protection afforded by the security container
- The position or site (Security Zone)
- The use of approved security equipment.

Incoming and outgoing materials at TOP SECRET must be recorded in a Classified Document Register. All TOP SECRET is ACCOUNTABLE MATERIAL and must track reference and copy numbers.

Printed material is immediately placed in a folder to prevent unauthorised access. Physical file folders for TOP SECRET material are red.

Audits must be conducted at irregular intervals. Personnel nominated to conduct spot checks are required to sight documents and acknowledge this in writing, This process should be carried out in conjunction with the owner of the information.

Electronic information is protected against illicit use or intrusion using two or more following mechanisms:

- Username / password or digital ID/Certificate
- Logging use at level of individual
- Firewalls and intrusion detection systems and procedures
- Server authentication
- Security measures specific to the operating system or application you use.

ICT media and systems holding TOP SECRET information must be in compliance with the NZISM.

Control and handling requirements

TOP SECRET

Use, copy or share

Information at TOP SECRET can be used in Zone 3 (Restricted Work Areas) or Zone 4 (Security Areas) but storage is not permitted. Refer to Store and File.

Clear desk policy is mandatory.

Emailing or transmitting of TOP SECRET information is not allowed across public networks and can only be transmitted using a system approved and accredited by the GCSB.

TOP SECRET information is ACCOUNTABLE MATERIAL by default. As such it requires:

- strict control over its access and movement,
- regular auditing, to ensure its safe custody.
- Once disseminated, it must not be copied or reproduced in any form.
- If additional copies are required, they must be requested from the original source.

All reproduced information must retain the original markings.

Conversations and meetings discussing TOP SECRET information must be held only in appropriate zone secured areas to prevent information compromise.

ICT media or equipment holding TOP SECRET information must be handled and used in compliance with NZISM 13 Media and IT Equipment Management, Decommissioning and Disposal.

Remove or transport

Removal of TOP SECRET information or equipment from your premises should be authorised by the originator or controlling organisation and in accordance with agency policy and basis of real need. For example, when going to a meeting.

You must not remove TOP SECRET information for short-term work at home without approval from the NZSIS and the originating agency (if not your own).

You must use security measures to protect marked information when it is in transit.

TOP SECRET information or equipment must be in personal custody of authorised individuals and kept in NZSIS approved container when being transported.

When moving TOP SECRET information or equipment within a single location

- Double envelope and use of an approved seal.

You have three options for manually transporting TOP SECRET information:

1. Dispatch through your transit system with hand-to-hand receipts at each stage of the journey.
2. Distribute within a building or part of a building that has been declared a specially-protected area – a Secure Compartmented Information Facility (SCIF). May be passed uncovered or via single opaque envelope provided it is transported directly between people with appropriate clearance and 'need-to-know' and there is no opportunity for any unauthorised person to view the information.
3. Carried via an authorised, security-vetted messenger in an NZSIS-approved briefcase, satchel, or pouch and transported directly to the authorised recipient.

When moving TOP SECRET information between locations within New Zealand

TOP SECRET material must be:

- Double enveloped
- Sealed with an approved seal
- Carried via an authorised, security-vetted messenger or safe hand courier.

When moving TOP SECRET information outside of New Zealand

TOP SECRET material must be:

- Double enveloped with a receipt from inside the inner envelope
- Sealed with an approved seal
- Carried via MFAT Diplomatic Safe Hand Courier Service – See MFAT for more information.