

Information Security

Table of Contents

Table of Contents	3
Introduction	5
Application	5
Principles	5
Legislation governing information	6
Related information	6
Security roles and responsibilities	7
Authorisation, clearances and briefings	7
Use of Information and Communications Technology (ICT)	8
No expectations of privacy	8
Your login QID and password	9
Police computers and smartphones	10
System integrity	10
Removable data storage media and devices	10
Bluetooth and other wireless communications	11
Repair and disposal	11
Disposal of computing equipment and media	11
Repair	12
Use of non-Police ICT	13
Personal devices	13
Cloud and other outsourced arrangements	13
ICT procurement and changes	14
Procurement of software hardware and IT related services	14
Changes to technology systems	14
The Internet and communications	15
Online access	15
Telephones	16
Telephone voicemail	16
Mobile phones	16
Radios	16
Secure telephone	16
Information classification and protection	17
Information management, storage and release	19
Information sharing, disclosure and redaction	19
Printing and scanning	19
Protecting where you work	21
Station and office security	21
Working away from Police premises	21
Applying for remote working	22
Travelling overseas	22
Reporting and managing information security incidents	23

Introduction

Application

This chapter applies to all users of Police information and ICT, including contractors and other non-Police users.

Reliable and secure information and technology is crucial to all day to day and long term Police activities and objectives. Easy access to timely relevant information enables us to be better placed to prevent crime and road trauma and to respond and resolve them more quickly. Most of us also access and use information and ICT services more frequently and diversely than at any time in the past.

Unauthorised and inappropriate use or a lack of security in relation to information, resources and technology, poses risks for Police, users and the public. Risks to Police include loss of capability, productivity and performance, inability to effectively carry out its functions and obligations, and loss of trust, confidence, and reputation. Risks to users include risks to their personal privacy and safety, breaches of duty and law, and disciplinary or civil action. Risks to the public relate to their privacy, safety and wellbeing, and their trust and confidence in Police.

The requirements and guidelines in this chapter are intended to help you to make best use of available technology and information whilst limiting the Police, the public and your own exposure to security risks.

Principles

Information security is a combination of protective, detective and responsive controls to mitigate risks associated with producing, handling and protecting Police information and assets. It includes measures relating to the confidentiality, availability, and integrity of information processed, stored and communicated by ICT and other means.

The guiding principles applied to information management privacy and assurance are:

- As a government agency, Police follows the Government's minimum security requirements defined in the [Protective Security Requirements \(PSR\)](#) and the [NZ Information Security Manual \(NZISM\)](#). The PSR outlines the Government's expectations for information, physical and personnel security. The NZISM details processes and controls representing good practice essential for the protection of Government information and systems.

Access is provided to systems equipment and information to help make your job easier and more effective but that is routinely based on trust rather than restrictive technical controls. It is expected that people use Police ICT and information responsibly in a manner that reinforces a professional image and reputation.

- We all ensure information is only used and shared for authorised purposes and is kept secure across all environments. Classified and sensitive information is handled in accordance with government requirements and situational risks. Information is managed in accordance with applicable legislation such as the Public Records Act and the Privacy Act.

Reasonable personal use of Police systems is permitted; but this is a privilege which may be altered if necessary. Such usage is at each user's own risk and may be logged and monitored.

Legislation governing information

The key legislation governing information use and management is:

- **Policing Act:** Under section 50 of the Policing Act 2008, a person commits an offence who without lawful authority or reasonable excuse, has in their possession any Police property, including Police information.
- **Privacy Act:** The Privacy Act 2020 mandates protection of personal information about any person. The Privacy Act establishes principles relating to the collection, storage, use and disclosure of information relating to individuals.
- **Official Information Act:** The Official Information Act 1982 applies to all requests made to public sector agencies for information that is not about the requestor.

Other legislation governing aspects of security, privacy and information management include:

- [Public Records Act 2005](#)
- [Criminal Records \(Clean Slate\) Act 2004](#)
- [Criminal Disclosure Act 2008](#)
- [Copyright Act 1994](#)
- [Anti-Money Laundering and Countering Financing of Terrorism Act 2009](#)
- Various other legislation also makes it an offence to access, use, distribute or publish offensive, objectionable or discriminatory material.

Related information

Specialist information security policies are available for:

- [Redaction and disclosure](#)
- [Sharing information with other agencies](#)
- [Working with information classified CONFIDENTIAL and above](#)
- [People managers](#)
- [ICT projects and service delivery.](#)

Related information is available in the [Departmental Security](#), [Privacy and official information](#), [Records management](#), [Criminal disclosure](#) and [Social Media](#) chapters, as well as [Our Code](#) and the [Ten-One Security and Privacy](#) pages.

Security roles and responsibilities

All Police employees, contractors and other service providers are responsible for providing and maintaining the security of Police resources and the resources of others in our care. Each role and contract may have specific, additional, responsibilities.

All staff must complete the basic security training course (Essential Security Awareness) and make themselves aware of the core security requirements relevant to their access and responsibilities. Non-staff with access to Police buildings and ICT should be provided with similar training and awareness.

The Police employees, committees and groups who have specific information security responsibilities are listed under [Roles](#).

Authorisation, clearances and briefings

All Police staff, contractors and other people with unescorted access to Police premises, information or other resources must be Police vetted. People with access to CONFIDENTIAL, SECRET or TOP SECRET information must also hold a current security clearance at the appropriate level.

Access to Police information is based on trust, rather than solely on the implementation of technical controls to block access. It is designed to improve day to day access to information. This is balanced by increased monitoring and compliance reporting, with the focus on early intervention, education and increased user awareness. It is also aligned to a higher expectation on employees and contractors regarding the appropriate use of information and technology.

Use of Information and Communications Technology (ICT)

Our information and ICT assets are of enormous value not only to Police but also to government and other agencies and, potentially, adversaries. All users of Police devices and computers should be aware of the security of such equipment and information, and take reasonable steps to avoid risk or compromise.

Physical access to Police ICT equipment must be controlled. This means keeping equipment in ways that minimise opportunity for unauthorised access, and challenging or preventing unauthorised people from using, or seeing information on, Police devices.

Adding or changing ICT services, software or hardware must be done via the ICT Service Centre. This includes purchases - including cloud services - connecting hardware, installing software, connecting to any non-Police network, removing equipment from Police premises, and disposing of equipment.

Police users provided with laptops, smart phones, or other portable devices, should be particularly careful to avoid loss or theft. Report lost devices to the Service Desk as soon as possible.

Users must not use or attempt to use another person's logon, or share mobility devices. Passwords, PINs, authentication tokens and all other Police data should be carefully protected from compromise.

In the event of any ICT security incident, all users should report the event immediately to their manager, and into SPIR ([Security and Privacy Incident Register](#)).

All Police employees and others with access to Police information and communications technology must ensure that in their use of the systems they take adequate measures to maintain:

- **Confidentiality of information:** Ensuring that information is not made available or disclosed to unauthorised individuals, entities, or processes.
- **Integrity of information, data and systems:** Protecting information from alteration or unauthorised destruction and preserving accuracy and consistency.
- **Availability of information and ICT services:** Implementing technology and processes so that information and services remain accessible and useable by authorised people.

The expectations on users of information and ICT is provided in the [Acceptable Use of Information and ICT policy](#).

No expectations of privacy

Users of Police technology and resources should not have any expectations of privacy of private communications made on, over, or through the use of Police systems. Business and personal or private information and communications may be subject to monitoring and review by being recovered and examined, with or without the knowledge and consent of the user. User activity is logged by various applications and equipment, including email servers and printers, and may be audited without notice. Police telephone systems, including mobility devices, are also subject to logging and reviewing of activity. This may include, for example, calls, voicemail, texts, emails and internet use.

Your login QID and password

Each Police user is assigned a unique QID (Police Query Identifier), which is used as the login ID for most Police systems. You are responsible for all activity undertaken using your login profile so be careful when selecting passwords and PINs, and protect them from other people.

Do	Don't
<ul style="list-style-type: none"> - Make passwords at least 10 characters long with a mixture of letters, digits, and symbols. Or if the system allows it make it 12 characters or longer just of letters or digits - Choose something unique and difficult to guess, but easy for you to remember without writing it down. Use the Police password storage app to keep track of multiple passwords 	<ul style="list-style-type: none"> - Don't use any words (or parts of words) associated with your identity as part of your password, including your QID, vehicle registration, position title, or names of any family members. Don't reuse Police passwords or PINs in other systems - If you need a written copy of a password or PIN, keep it in a secure place that is not close to any device that it is used to unlock.

Tip: Use mnemonics phrases or simple melodies to help you remember complex passwords easily

Do not attempt to use another person's login, or let another person to use your login profile, unless for a short time and under your supervision. Do not share your login passwords or PINs with any other person. If you do get in a situation where someone else might know your password or PIN, change it as soon as possible.

Police computers and smartphones

Staff are responsible for the physical protection of any laptops, phone and other devices issued to them whenever the device is outside Police premises.

Follow these instructions to ensure that as a user, you are taking all reasonable measures to protect ICT devices and information.

Condition	Computer security instruction
If possible	Enable the password-protected screen saver, to automatically start within 15 minutes of inactivity for computer and 5 minutes for smartphones
Computer or smartphone is left unattended temporarily	Lock the device e.g. Ctrl Alt Del
Computer is likely to be unattended for an hour or longer	Log off
Undocked portable computer	Power off and, if applicable, ensure the remote access authentication (RSA) token is kept separately

System integrity

Do	Don't
<ul style="list-style-type: none"> - Recommend to ICT that useful software be considered for authorisation, and apply via the Service Desk to request particular access that is blocked by controls. - Be cautious of suspicious emails, attachments, and links. Notify the Service Desk immediately of any suspicious activity or suspected system infection. 	<ul style="list-style-type: none"> - Install or run unapproved software on any Police system. - Attach additional hardware, peripherals or other devices to a Police device or network, without specific authorisation from ICTSC. - Interfere or attempt to circumvent security measures or access controls on any Police device or system.

Note:

- Attackers can disguise the source of emails, so being vigilant doesn't just apply to unknown addresses.
- Malware sent in email attachments will often be disguised, such as having two or more file extensions (e.g. filename.jpg.exe).

Removable data storage media and devices

Removable data storage media (i.e. optical disks, USB flash drives, camera memory cards, portable hard drives) and devices may be used but the risks of malware infection and accidental information disclosure must be managed. You may use them for work purposes without having to request access, but you should:

- scan media for viruses before or as soon as you use it in a Police device
- wherever possible, encrypt media that could be taken out of the Police environment to ensure that if it is lost, whoever finds it will not be able to access the data. If you only want to read files on a USB device, you do not need to encrypt it.

In situations where the media cannot be encrypted, it should be marked with an indication of the content and its classification, if any.

Once encrypted, locked media containing SENSITIVE or RESTRICTED information only needs to be protected as an IN CONFIDENCE item. USB devices only need to be set up for encryption the first time you plug them into the Police network. All files already on these devices will be automatically encrypted once the process is complete. Instructions are available from the Service Desk.

Bluetooth and other wireless communications

Bluetooth is a popular technology that interacts with computer peripherals such as printers, smartwatches, headphones, vehicle infotainment systems and data storage.

Bluetooth is disabled on Police laptops and desktop computers.

Bluetooth and other peer-to-peer networking may only be used with other Police devices in the following situations:

1. Where the device type and/or configuration has been pre-approved by the CISO or IT Security Manager. The only currently approved usage is:
 - a. Connection of a Police mobile phone to a Police vehicle's onboard infotainment system. Full pairing of a Police mobile phone to rental or personal vehicles is **not** allowed, nor is pairing of a personal device to a Police vehicle.
 - b. Personal or Police issue wireless headphones and hands-free telephony may be used if the link cannot share stored information such as address books **or**
2. Mobility apps with Bluetooth that have been approved via ICTSC's assessment process.

Where wireless functionality is enabled, those devices must be configured to reject all unexpected pairing requests and, where possible, be set to be undiscoverable except when being paired. The networking functionality should be turned off when it is not needed.

Repair and disposal

Disposal of computing equipment and media

Special care is required to ensure there is no possibility of official or personal information being retrieved from media, devices and other equipment once they are out of Police control. Therefore, all Police ICT equipment (including cellular phones) must be disposed of only through the ICTSC.

Devices must be purged of all information using a deletion utility program approved or compliant with the standards in the NZISM and provided by ICTSC. Alternatively, the storage media should be destroyed (e.g. by shredding). In some situations where the media is encrypted, ICTSC may use alternative methods to ensure the content cannot be recovered.

Removable storage media must have the contents deleted (standard delete or reformat function) and, if not wanted for re-use within Police, the media must be destroyed (e.g. shredded) or disposed of through a secure waste contract [s.6\(a\) OIA](#). Storage media used at any time to hold Police information must not be sold or given away unless it has been sanitised via a method approved by the IT Security Manager.

If (non-smart) mobile phones cannot be reimaged, at least ensure all contact and call information is deleted and cannot be recovered.

Repair

Police computers, devices and telephones (including mobile phones) must not be taken for repair or service by people or companies other than those approved by ICTSC. If the functioning of the equipment makes it possible and practical, information should be deleted before access by repair service people.

Service providers should be required to sign a non-disclosure agreement in respect of any information retained on the equipment under repair, or received incidentally during their visits to Police sites.

Use of non-Police ICT

Personal devices

Personal devices, such as laptops and smartphones, must not be connected into the Police network. Sensitive Police information must not be stored or processed on any non-Police devices unless with prior approval from the CISO or IT Security Manager. Only ICTSC approved peripherals such as mice and keyboards may be connected to Police devices. For example, Police laptops are not to be connected to home and other non-Police printers.

Cloud and other outsourced arrangements

Police information planned for outsourced or offshore ICT arrangements must be notified to the CISO. The security Certification and Accreditation process is likely to be necessary to ensure security risks and requirements are adequately managed.

ICT procurement and changes

Procurement of software, hardware and IT-related services

All software used by Police must be authorised, certified and installed or modified by the ICT Service Centre or an ICTSC-approved outsource vendor. All other software is prohibited and must not be installed onto Police technology.

Only employees, contractors and other third-party users authorised by the ICTSC may modify software or software configuration. This includes anti-virus software, which must remain operational as installed and configured by ICTSC.

Software may only be used for the purpose for which it is intended, e.g. word processing, spread sheeting etc. It must not be copied or used outside the license agreement.

Police hardware must be procured, certified and supplied by ICTSC, including any technology equipment that:

- connects to the Police network, such as laptops, printers, PCs, mobile devices
- is used to deliver voice or data services to staff, such as telephones, mobile phones, etc.

ICT hardware is labelled with a Police inventory identification number. This label should not be tampered with.

Changes to technology systems

All employees may:

- connect or disconnect Police-supplied docking stations, monitors, portable printers, keyboards and mice to laptops
- move laptops, or connect or disconnect them from the network
- replenish computer consumables.

However, only authorised agents such as ICTSC employees or contractors authorised by the CIO may make material physical changes to components of Police technology systems (e.g. relocating desktop computers, adding a new computer to the network or installing software).

The Internet and communications

Online access

Police provides access to Internet websites and information - including social media - for work and reasonable personal use from Police ICT devices. That access is subject to:

- restrictions on sites or content that are suspected of containing dangerous, inappropriate or objectionable material. Exceptions may be justified and approved through a request to the Service Desk in some circumstances
- logging and review of the sites and pages visited, with the generation of alerts if a user attempts to access prohibited sites
- interacting publicly in accordance with the [Social Media policy](#).

The Internet is an unsafe environment, so all reasonable steps must be taken to prevent:

- unauthorised disclosure of Police information over the Internet
- the introduction of malware or vulnerabilities into the Police environment.

Only use the Internet in line with the [Code of Conduct](#), [Acceptable Use](#) and the [Social Media policy](#). For instance, do not (non-exhaustive list):

- access sites or disclose information that exposes systems or official information to unauthorised access or increases the risk of such access
- access material that is sexually explicit, racist, abusive or otherwise offensive, unless such access can be demonstrated as being required in your work
- perform online gambling
- knowingly subscribe to services or distribution lists that could result in frequent or large messages that interfere with Police or ICT performance.

Be careful when using public services such as social media that you do not (unless expressly authorised):

- identify yourself as a Police employee
- release official information
- express views that may be interpreted as being the Police view.

Follow the guidance for sending and managing [emails and texts](#).

Telephones

Police business relating to unclassified and IN CONFIDENCE matters may be discussed by telephone of any type. SENSITIVE or RESTRICTED matters may be discussed when both callers are on the Police internal (Voice over IP) telephone network. Otherwise, take particular care and use guarded language and guarded references whenever possible.

Consider the risks of interception and overhearing when discussing private or operationally sensitive information over the telephone or conferencing systems.

Telephone voicemail

Most telephone message systems are intrinsically vulnerable to hacking so voicemail should not be used for sensitive messages. Change the access PIN as soon as possible after being allocated a new telephone number.

Mobile phones

Mobile networks offer some security if both callers are using the same digital phone network. However, as number portability between Vodafone and Telecom now exists, the number is no longer a reliable indicator that callers are on the same network (e.g. a 021 number could be on either network). Depending on the nature, scale and security risk for any particular operation, assume that a digital mobile call can be overheard or intercepted so be careful where and what you discuss.

Radios

Operational staff should use encrypted digital radios whenever possible to protect information. Where encrypted radios are not available (e.g. where analogue radio is still used), note the potential to be overheard or intercepted and therefore be guarded on the nature of information to be disclosed.

See also the policy concerning [third-party access to the Secure Digital Radio Network](#).

Secure telephone

Police provide secure (encrypted) telephones to secure voice communications for classified information. They can also be used in normal or insecure mode, so make sure they are operating in Secure Mode with a compatible phone at the other end before discussing anything of a classified nature.

Information classification and protection

Information is one of the most valuable tools to Police, and it is often entrusted to us by other parties, so it is important that we respect its significance and take all reasonable steps to protect it. Information should only be accessed when needed, and handled carefully in accordance with law and Police policy.

‘Need to Know’ is a fundamental security principle. The only people who should receive classified information are those who need it to perform their duties. It does not include ‘nice to know’ or ‘convenient to know’, and should not be provided merely by virtue of position, rank or clearance level.

The ‘Release’ principle - enshrined in the Official Information Act - balances ‘Need to Know’. Official information should be made available to the public unless there are good reasons to withhold it. Classification is not by itself justification for withholding information if it is requested: the criteria in the Act must be applied. The national security classification system takes account of the statutory criteria.

All information held by Police must be:

- only made available to people who have a legitimate ‘need to know’, or subject to policy
- only accessed if there is a legitimate need to do so, especially if it is personal information
- handled carefully, especially when it is being carried or sent outside Police premises
- released only in accordance with legislative requirements, directives of the Government or Courts or Police policy.

Security classifications help guide this appropriate treatment of information. Information may be classified if its dissemination could be damaging to the interests of individuals, groups, commercial entities, government business, the community, or national security. The definitions of each level of classification are based on escalating consequences of compromise.

The government National Security classifications are RESTRICTED, CONFIDENTIAL, SECRET, and TOP SECRET. These may only be applied to information which has bearing on New Zealand’s security and diplomatic relations. The Policy and Privacy classifications (those that do not relate to national security) are IN CONFIDENCE and SENSITIVE.

Almost all Police official information is either unclassified, IN CONFIDENCE, SENSITIVE or RESTRICTED, and all Police employees, contractors, and third parties who have successfully completed the Police vetting and validation process are approved to apply these and access classifications if their duties require it. A government security clearance at the appropriate level is required for access to CONFIDENTIAL, SECRET and TOP SECRET material.

Protected information may also be endorsed by other markings that indicate a special level of care. These usually relate to the specific nature of the information, temporary sensitivities, or limitations on availability, circulation or access.

Public information or other information that does not reach the threshold for IN CONFIDENCE information may be marked as “Unclassified” to indicate that an assessment of the information has taken place. This

practise removes any assumption regarding the classification of the information. While unclassified information may not require the same level of protection as IN CONFIDENCE information, security controls may still be justified to protect its confidentiality, integrity and/or availability.

For minimum standards for protecting and handling information see [Classification and minimum protection standards](#).

Information management, storage and release

All information collection, use and management must satisfy the Public Records Act, the Official Information Act, the Privacy Act, the Criminal Disclosure Act - for disclosure of relevant information between the prosecution and the defence - and, where applicable, any Court directives.

It is important that Police ICT applications and services are designed and operated to satisfy their information management requirements, but a lot of Police information is also stored and managed outside those structured services.

- s.6(a) OIA

Use the ITSM Self Service forms to manage the items above.

Information sharing, disclosure and redaction

Personal or classified information shared between Police and any other agency must be protected and managed to ensure legal requirements and security risks are addressed. Guidance on developing formal agreements is available in [Police Interagency Agreements Policy](#). Additional security guidance is provided in [Sharing Information With Other Agencies](#).

Prosecution and Legal's [Privacy and Official Information](#) chapter provides guidance on balancing the need to share information with Police obligations to withhold information.

Electronic documents and other formats often contain non visible information like hidden fields and track changes increasing the risk of inadvertently leaking unintended information when sending or releasing those files outside Police. Information that is redacted incorrectly might also be trivial to recover. The rules and protocols are covered in the [Electronic Redaction and Disclosure policy](#)

Printing and scanning

When printing or scanning documents, follow the security advice in the table to minimise the risk of information loss or being accessed by unauthorised personnel.

Secure print	The secure print service requires users to log on to multi-function devices, using an access card, prior to printing documents. It reduces the risk of printed documents being picked up in error by somebody else, so it should be used where available.
Scan to email	Most Police users can direct scanned documents to be sent to their Police email account. Where this option is available, it should be used as the preferred scanning method.
Scanning documents to network folders	Multi-function devices provide the capability to scan documents and load them directly to a folder on the Police network. The scanned document folders can be accessed by all Police users, which might result in unwanted access. To reduce this risk, use the scan-to-email function instead, or copy the scanned images to a secure or personal folder, then delete them from the scanned document folder.

Contact the Service Desk for further information on any of these functions.

Protecting where you work

Station and office security

Site physical security measures are in place in all Police premises to protect equipment from theft or damage. They should include:

- staff and visitor identification and access control
- video surveillance
 - out of office lock up routines
- monitored intrusion detection and environmental systems
 - the housing of sensitive information and ICT equipment in secure rooms and/or lockable cabinets with access restricted to specifically authorised personnel
- a review of security whenever equipment is moved to another location or a site is rebuilt or modified.

Sensitive material should not be left on your desk when you are not there. Keep it in locked cabinets or drawers to prevent unauthorised or accidental viewing. Desks should be kept as clear as possible when not in use.

Laptop, desktop and smartphone screens should be locked when unattended.

Also consider the location of displays keyboards and printers and the chance of an unauthorised person seeing the screen a password being entered or sensitive hardcopy documents Printers should be configured for Follow me printing (i e secure print)

Working away from Police premises

Remote working is work involving official information - which would normally be done in Police premises - being carried out at home or another location for an extended period of time.

Special considerations are required as remote working can increase the risks of:

- compromise of Police information
- loss or damage of equipment if it is transported to and from home and office
- inadvertent introduction of malware (e g viruses) to the Police environment

The degree of risk increases with the sensitivity of the information being worked on and the length of time the remote working is conducted If the option is taken because of convenience for the employee this may be offset by the right of Police as employer to be assured about security

All premises used for storage or processing of unencrypted Police SENSITIVE or RESTRICTED information must be certified by Protective Security.

When remotely accessing the Police network:

- protect the computer storage media and hardcopy from theft
- connect to the Police network remotely using your encrypted Police laptop

- log off when you leave the device or are not using the network
- ensure any external storage used is encrypted.

Do not send Police information to your personal computer or email accounts or send passwords or other authentication information via email.

Applying for remote working

Remote access to the Police network is available through Police-provided and configured laptops and smartphones via a Virtual Private Network (VPN) secure channel between your device and a secure access point on the Police network. You log into the Enterprise system with your QID and enterprise password **s.6(a) OIA**

You can apply for remote access if you need to work away from a Police station or office. The [Police flexible working policy](#) may also allow you to work from home or an external office. 'Full' or 'Partial' remote access to can be provided depending on your situation. Remote working involving any classified or operational material must be approved by a Superintendent or higher. Advice may be obtained from the Service Desk or Manager: Protective Security. More information is available in the [Remote Access page](#).

Remote access authentication tokens must:

- be protected from compromise
 - be removed from the work area at the end of the working day and safeguarded by the user
- not be left with a laptop unless it is under direct supervision of authorised users.

Lost remote access tokens should be reported to the Service Desk as soon as possible.

Travelling overseas

If it can be avoided, do not take Police laptops or smartphones out of Australasia. **s.6(a) OIA**

Reporting and managing information security incidents

This section provides an overview of the process to report and manage ICT and information security incidents, including:

- accidental or unauthorised access to official information
- inappropriate use of Police technology
- attempted penetration of the Police network systems or cloud services
- infection by malware
- intentional denial of service (DOS)
- damage, loss or theft of a device or computer equipment
- unauthorised physical access to Police information or equipment

When a security incident occurs it is crucial to report and manage it quickly and with appropriate rigor to minimise the damage it causes to the affected assets as well as NZP objectives and obligations

The priorities are to:

- prevent further loss or damage
- preserve evidence if an investigation may be needed
- ensure the appropriate managers and stakeholders are kept informed.
- notify other staff and/or the public if the incident is likely to escalate, spread or continue.

If the incident involves accidental disclosure of information, attempt to have the unwanted copies of the information deleted to limit its exposure. Should personal or official information be inadvertently released or other inappropriate access or use occurs, then it is vital that the incident is managed quickly and appropriately.

Incidents need to be reported through the [Security and Privacy Incident Register](#) (SPIR). Reporting them immediately can help to reduce the damage and ongoing risk. The SPIR system will ensure that the applicable District Operations Manager and the specialist Protective Security, Privacy and Cybersecurity teams are informed.

Depending on the situation, you may also need to notify one or more of:

- the Service Desk for any security matters to do with ICT systems or services. The Service Desk will contact Cybersecurity and other ICT specialist teams as necessary.
- Police Professional Conduct if it involves a breach of Our Code
- Legal Services if it involves a legislative breach
- Police Prosecution Services if it involves a criminal disclosure matter
- Public Affairs if it involves a matter of media interest
- High Tech Crime Group if it concerns cybercrime.

The general phases for security incident handling are (note, they can occur in parallel):

- Identification: This phase deals with the detection and determination of whether a deviation from normal operations needs to be handled as a security incident. It also involves assessing the scope of the problem and triaging how it will be handled.
- Containment: The primary purpose of this phase is to respond quickly to limit the damage and prevent any further damage from happening. It may also include system back-up to preserve evidence. For ICT security incidents that are potentially a targeted attack:
 - collect relevant artefacts, logs and data, and remove them for further analysis
 - implement mitigation steps to stop further spread or damage while avoiding tipping off the adversary that their presence has been discovered
 - consider obtaining additional incident response support from NCSC, CERTNZ, High Tech Crime Group and/or a specialist incident handler to provide additional expertise and technical support to the incident response.

Eradication: This phase deals with removal of the threat from the environment and restoration of affected information systems and services to a known good state

- Recovery: The purpose of this phase is to bring the affected systems and services back into production in such a way that it will not lead another incident. It is essential to test, monitor, and validate the systems that are being put back into production to verify that they are not still vulnerable to the same or similar threats. It might also include further investigation and/or a post-incident review to reduce the risk of follow-on problems or incidents.

Activities around victim notification, media relations and criminal investigation may also be needed throughout all phases.

Any privacy breach that could cause or have caused serious harm to an affected individual or individuals, or is likely to do so, must follow the [Privacy Breach Management process](#) and be reported to the Office of the Privacy Commissioner and the affected individual(s) as soon as practicable after becoming aware that the breach has occurred.

Large privacy or security incidents should be managed in consideration of [TENR](#) in a similar way to a large investigation or a [CIMS](#) incident:

- agree an Incident Manager. The Incident Manager must manage the incident to its resolution, including involving the relevant stakeholders above
 - assign other key roles such as: Business Representation; Communications; Legal; Investigation; Response; Recovery; Privacy; Security; Information Management
- establish a log of events and associated information management
 - schedule regular incident management meetings with all key contributors
- provide scheduled and/or milestone updates to stakeholders, including the Chief Security Officer and Media Relations
 - for incidents involving ICT adopt the ICT Incident Management Process

Where applicable incident liaison will also need to be established with the following authorities:

External party	NZP liaison point
Office of the Privacy Commissioner (OPC)	Chief Privacy Officer
Government Chief Privacy Officer (GCPO)	Chief Privacy Officer
Government Chief Digital Officer (GCDO)	Chief Information Officer
State Services Commission	Director Assurance
Government Chief Information Security Officer (GCISO)	Chief Information Security Officer
Computer Emergency Response Team (CERTNZ) and the National Cyber Security Centre (NCSC)	IT Security Manager

Liaison points with other parties and sectors may also need to be included in the incident management structure depending on the nature and scope of the incident (e.g. Five-Eyes Law Enforcement Group via the FELEG SPOC).

Printed on : 30/05/2022