Managing security risks in policing

Table of Contents

Executive summary

The Commissioner has ultimate responsibility for:

- assuring the implementation and management of effective protective security governance within Police to protect its personnel, physical and information assets
- annually certifying that Police meets its Protective Security Requirements (PSR) mandatory obligations.

Key critical points

Police must ensure the New Zealand Government Protective Security Requirements (PSR) are implemented and maintained for governance and managing personnel, physical and information security:

- The Deputy Commissioner: Strategy and Service is Police's Chief Security Officer, and is responsible and accountable to the Commissioner for overseeing the management of protective security across Police, and ensuring protective security of operations, practises, procedures and policies are aligned with the government's PSR framework.
- The Security and Privacy Reference Group (SPRG) is the specialist governance body chaired by the Chief Security Officer. The SPRG applies national oversight of the PSR within Police, providing pathways for successfully and appropriately protecting Police people, information and assets.
- All employees are responsible for managing and reporting safety and security risks. The three lines of defence model enables staff to apply at least one level of defence to remediate risk to an acceptable level.
- The Protective Security Workbook assists Districts, workgroups and Service Centres to assess and record their progress towards meeting their protective security objectives and achieving security maturity and identify ways in which capability could be lifted.
- The Commissioner's independent Assurance and Risk Committee (ARC) reviews risk management and mitigation processes, internal control procedures and compliance with relevant statutory and regulatory requirements.

Overview

Introduction

Effective security enables Police and partner organisations to work together securely in an environment of trust and confidence.

Protecting Police people, information, and assets helps meet our strategic and operational objectives.

Protective Security Requirements (PSR)

The PSR outlines the Government's expectations for managing personnel, physical and information security. It includes mandatory requirements that Police and other agencies must implement to ensure a consistent and controlled security environment throughout the public sector.

For further information about the PSR, see:

- Annex 1 - PSR Mandatory requirements in this part of the 'Departmental security' chapter for a summarised list of the 20 mandatory requirements
- http://protectivesecurity.govt.nz.

Compliance

All Police employees, contractors and service providers must comply with the requirements of the 'Departmental security' and the 'Information security' chapters.

Legislation

The security and safety of all New Zealanders are implicit in the purpose of Police, as exemplified by the solemn undertaking taken by all employees, and constabulary oath.

Security and safety is also in most legislation relevant to conducting Government business. Examples include:

- The Commissioner must provide a safe working environment (Health and Safety at Work Act 2015)
- Mandated procedures for financial management (e.g. Public Finance Act 1989)
- Guidelines for releasing official and personal information, and protecting it where warranted (Official Information Act 1982)
- Guidelines for the release of personal information and the protection of it where warranted (Privacy Act 2020).

Table of definitions

For the purpose of this chapter:

- 'District' includes PNHQ, Service Centres and business groups
- 'Police employee' includes all staff employed under section 18 of the Policing Act 2008
- 'Service provider' includes Contractors, Workers engaged by NGOs who perform work for Police, Secondees, Interns and Volunteers.

See ‘Information security roles and responsibilities’ for detailed information about people who are engaged by Police.

Protective security governance

The Commissioner has ultimate responsibility for security of Police people, information and assets by:

- assuring the implementation and management of effective protective security within Police by meeting the PSR Mandatory requirements
- certifying the New Zealand Government annual security self-assessment and providing the compliance reporting to the Government Protective Security Lead (GPSL).

Chief Security Officer

The Deputy Commissioner: Strategy and Service is the Chief Security Officer for Police responsible and accountable to the Commissioner:

- for protective security in Police
- ensuring protective security of operations, practises, procedures and policies are aligned with the Government's framework for security, detailed in the PSR.

Security and Privacy Reference Group (SPRG)

The Security and Privacy Reference Group (SPRG) is a steering group chaired by the Chief Security Officer. Membership of the group includes:

- Executive Director: Service and Resolutions
- Chief Information Officer
- A representative District Commander
- Director: Infrastructure
- Director: Assurance
- Chief Privacy Officer
- Manager: Protective Security/Chief Information Security Officer.

The SPRG applies national governance of the PSR with the understanding it provides pathways for successfully protecting people, information and assets at PNHQ and Districts to:

- better manage business risks
- assure continuity of service delivery
- assure annual security self-assessment against mandatory requirements of PSR is accurate
- assure the Government and the public that Police have appropriate, effective measures in place to protect New Zealand Police people, information and assets
- recommend certification annually to the Commissioner of PSR compliance.

See 'SPRG' for information about the group's roles and responsibilities.

PNHQ group governance

Directors are responsible for the development, maintenance, review, performance and compliance of PSR

within their group or Service Centre.

Protective security roles and defined responsibilities for each area must be appointed and established as points of contact.

It is best practice for protective security to be a standing agenda item at Directors' leadership team meetings.

District governance

District Operations Managers are the District representative responsible for the development, maintenance, review, performance and compliance of PSR within their district. Points of contact with protective security roles and defined responsibilities for areas within a district must be appointed.

It is best practice for protective security to be a standing agenda item at District Leadership Team meetings.

Annual security assessment

It is a Cabinet requirement for the Commissioner to provide an annual self-assessment detailing Police's progress with meeting the PSR mandatory requirements, and how security improvement initiatives are being applied. The Commissioner endorses the assessment by certifying that the Police submission is a true and accurate representation of the protective security condition across the organisation.

Education about the PSR

Police must provide all employees, contractors and service providers with sufficient information and security awareness training to meet the obligations of the protective security requirements.

A common base level of security awareness is achieved through the mandatory completion of the Essential Security Awareness module in MyPolice. The module must be completed every two years.

See 'Security awareness learning' in 'Personnel security' of the 'Departmental security' chapter.

Procedures for reporting and investigating security incidents

Police employees and service providers must be aware of established procedures for reporting and investigating security incidents. Procedures are verified in agreements and protocols between:

- PNHQ's Professional Conduct Group and the Principal Adviser: Protective Security
- District Professional Conduct Managers and the Principal Adviser: Protective Security.

See 'Personnel security' for guidance with:

- educating employees about security
- responsible behaviour
- travel information security
- conference security
- security incident response

- investigating a security incident.

District Commanders and other district managers must ensure that Police employees and service providers who are likely to handle classified information derived from or provided by partners are aware of their obligations to protect the information in accordance with the providers direction.

Business continuity management (BCM) programme

The BCM programme is established to provide for the continued availability of critical services and assets warranted by a security threat or assessment. The programme consists of the development and maintenance of business continuity plans of:

- critical services and assets
- information exchange priorities with other agencies
- ensuring currency, testing and two-yearly reviews.

Security principles

Definition of security

An organisation's security is the range of methods used to protect people, assets, operations, information and reputation from harm or loss inflicted through human factors, whether intentional or inadvertent.

Security overlaps with other areas of organisational management such as professional ethics, tactical training and managing intelligence.

Security measures

Security provides protection through:

- personal safety awareness
- physical barriers and constructions
- installed deterrence and detection systems (alarms and CCTV etc)
- employee integrity assurance (employment vetting and screening)
- procedures for protecting information
- maintaining discretion about operations, tactics and plans
- controlling access to information and communications technology
- investigating and responding to security incidents
- sensible administrative procedures, practices and training.

See 'Security measures' in this part for guidance with planning and applying a combination of security measures.

Context for security

Effective security should be an integral part of Police business. When good security is routine and normal it enhances our ability to our job. It also gives the public and stakeholders confidence and assurance that their interests are met and that information is protected.

The Commissioner must ensure Police employees work in a safe and secure environment - to the greatest extent possible - and all Police employees have obligations to act as responsible stewards of publicly-funded assets. Furthermore, government has specific requirements about ensuring the confidentiality, integrity and availability of both its own official information (any information developed, received or collected by or on behalf of the government) and New Zealanders' personal information which is held by Police.

Government policy

Cabinet directive

In December 2014 Cabinet approved the Protective Security Requirements.

See 'Annex 1 - PSR_Mandatory requirements' for more information about the PSR.

The PSR incorporates the New Zealand Information Security Manual (NZISM), which contains the New Zealand Government's standards for information systems security.

Interdepartmental security policy committees

Interdepartmental committees develop Government sector security policies and guidelines. The principal committee is the Officials Committee for Domestic and External Security Co-ordination (ODESC), comprising the chief executives of government agencies who have security and intelligence responsibilities.

Within the ODESC structure several committees exist with these committees having responsibilities for intelligence and policy matters.

The ODESC sub-committees are:

- Interdepartmental Committee on Security (ICS)
- Government Communications Security Committee (GCSC).

Security risk standards

Applicable New Zealand and international standards and guidelines include:

- AS/NZS ISO31000:2009 Risk Management - Principles and guidelines
- ISO/IEC 27001:2013 Information Technology - Code of Practice for Information Security
- SA/SNZ HB 89:2013 Risk management - Guidelines on risk assessment techniques
- SA/SNZ HB167:2006 Security risk management.

Police security policy

In accordance with the PSR, Police protective security policies, plans and protocols must be developed and then reviewed every two years to meet the organisation's specific operational and business needs.

Applying the policy

Protective security policy applies to all Police employees and service providers; and, in respect of all use of or access to Police resources, equipment and information.

What is the policy's scope?

Protective security policy addresses all elements of the security definition and in addition it specifically addresses issues of the propriety of collection, retention and use by Police employees, contractors and service providers of personal information.

There is an overlap between the measures intended to keep people safe from accidents and natural disasters, and those that deal with harm caused by others.

The policies and procedures flowing from the security related chapters of the Police Manual may mandate minimum content and best practise for certain types of security threats, but will not replace published emergency procedures specifically written for each building or location.

This table shows the security policy's scope.

Our security policy…	The policy does not…
- includes all elements of the definition of security - aligns and complies with the PSR - specifically addresses the Police collecting, retaining and using personal information - may mandate minimum content and good practice for responding to some types of threats (for example bomb threats and suspicious mail) - covers using Police information and communications technology systems - includes all elements of the definition of security - supports business continuity and disaster recovery - regardless of what caused the disruption.	- replace published emergency procedures specifically written for each building or location - cover specific Police health, safety and wellness policies, though physical security measures must be consistent with H&S legislation - cover bullying or harassment in the workplace - cover denial of opportunities in the workplace - include more technical aspects of ICT security which are intended to guide design and management of ICT systems.

Related security policy

Further guidance relating to security policy is available in other Police Manual chapters. For example, see:

- 'Cash handling' for when handling cash in various situations, such as when cash is seized with or without warrant; held as an exhibit, or for safekeeping (e.g., as the property of a deceased person); or received as found property.
- 'Civil defence and emergency management' (CDEM) for policy, principles and procedures applicable to planning for Police control of emergencies or disasters and, where necessary, the passing of control to the CDEM organisation in the event of a declaration of a state of emergency.
- 'Code of Conduct' for information about the standards of behaviour expected of all Police employees.
- 'Community disclosure of offender information' for information about the criteria for disclosure, what information may be released and the authorisation that must be obtained.
- 'Criminal disclosure' for policy, process and procedure about criminal disclosure and includes key duties and responsibilities for Police employees.
- 'Departmental security' for information about the range of security measures in place to protect Police people, assets, operations and reputation from harm or loss inflicted through human factors, whether intentional or inadvertent.
- 'Privacy and official information' for an explanation about the law you must consider before deciding whether or not to disclose information.
- 'Elections and political matters: a guide for Police employees' for guidance about releasing offence statistics and all media and Official Information Act requests about electoral related offending.
- 'Financial' for information relating to finance policies and procedures in Police.
- 'Improvised explosive devices and bomb threats' for information on improvised explosive devices (IED) types and characteristics, and the role of Police in IED emergencies and IED procedures, and provides advice that should be given to organisations that may become targets of IED attacks.
- 'Information security' which provides governance structures for security of information and acceptable use policies, standards and procedures; risk management processes to assure the design and operating effectiveness of the security information practices; and certification and accreditation of systems.
- 'Fraud and corruption' for policy and principles for the management of internal fraud, theft and corruption allegations.
- 'Managing conflicts of interest' for rules about providing written character references.
- 'Missing persons' for information about media broadcasts of the personal details, circumstances and images of the missing person.
- 'Monitoring and using publicly accessible social media networks' for details about Police use of publicly accessible social media sites and operating principles.
- 'News releases' for guidance about how much information to release.
- 'Police investigations of complaints and notifiable incidents' for reporting and investigation guidance of serious misuse of technology and equipment from an internal source.
- 'Police response to cyberbullying and the Harmful Digitial Communications Act' for information about NetSafe, Spark, Vodafone and complaint investigation processes.
- 'Information and records management' for policies and processes for records management in Police, good record keeping practices and information on file retention and disposal.
- 'Releasing information to the media' for guidance on releasing information and having authorisation to speak to the media (including after sudden death cases).
- 'Sub-judice' for guidance about information not to be released.

- 'Unacceptable behaviour - Kia Tū policy and guidelines' for information about how to report matter of integrity being compromised.
- 'Wanted persons postings' for information about:
    - when images may be posted
    - verifying information before it is posted
    - processing the image
    - posting on Facebook.

Security strategy and planning cycle

Purpose

The security strategy and planning cycle ensures ongoing review, evaluation and, if required, changes to security standards in Police.

Phases

The security strategy and planning cycle has four distinct phases with each dependent on each other. They are:

- Planning and development
- Delivery resources
- Response and prevention
- Monitoring and review.

Planning and development

This phase contains the development of the Police security strategy which outlines the overarching, strategic goals and objectives and identifies key security risks. The strategy guides the development of specific action plans, and policy, standards and guidelines in respect of security.

Delivery resources

It is important that Police integrate risk management into all decision making. The risk cycle will sit alongside the business plan; it will enable managers to:

- analyse, identify and manage their risks
- support decision making and good governance
- differentiate what is business as usual and what needs to be put into the business plan
- identify resource decisions
- establish clear expectations about how business units intend to integrate security risks into their management approach in both short and long term.

Advice on security matters can be sought from the Principal Adviser: Protective Security.

Strategic action plans (response and prevention)

The strategic action plans are derived from the requirements set out in the Police's security framework. The plans will help Police ensure risks are identified and appropriately managed.

Monitoring and review

The policy review process should be triggered by any changes affecting the basis of the original risk assessments. Risks might include:

- significant security incidents

- the introduction of new vulnerabilities
- changes to the Police organisational or technical infrastructure.

Monitoring and review is an ongoing cycle of:

- prioritising assets and vulnerabilities
- assessing the effectiveness of our security advice and awareness
- monitoring our security measuring and taking note of lessons learnt from incidents or breaches.

Security risks to Police

Internal vulnerabilities to external risks

Police internal vulnerabilities to risks from external sources include:

- Compromising politically sensitive information
- Theft, burglary and fraud
- Corruption, destruction, or unauthorised access to computer data
- Criminal damage
- Natural disaster.

Compromising politically sensitive information

Criminal groups, foreign state-sponsored agencies and individuals, and other private groups and individuals are known to attempt to obtain personal and other sensitive information from government agencies for a range of reasons, including personal, professional, or political gain. For this reason it is important Police are aware of and able to manage the risk of accidentally disclosing information to those who are not entitled to it, and the risk of internal threats who may deliberately disclose information

Theft, burglary and fraud

There is a growing threat of theft, particularly of information technology equipment. Arms, ammunition and explosives are always at particular risk.

Theft may occur through burglary or the actions of dishonest employees or service providers. Establishments responsible for collecting or disbursing public funds are susceptible to fraud and there is an increasing threat of fraud through manipulating IT systems.

Corruption, destruction, or unauthorised access to computer data

The integrity of data held on computer systems may be compromised by disaffected employees or service providers.

Police employee programming expertise, ready availability of malicious software (e.g. viruses) and the ease with which it can be deliberately or accidentally introduced, combine to create a substantial threat.

Criminal damage

Criminal damage can be carried out by employees, dependents, visitors or intruders. Criminals may also act, either knowingly or unknowingly, on behalf of political- or issue-motivated groups.

Natural disaster

Natural disasters are risks to the integrity or availability of facilities, buildings or equipment etc. They can be caused by incidents such as earthquake, fire, flooding, subsidence, or lightning strike.

National security clearances

An employee's suitability to obtain a national security clearance can be harmed by the external risks outlined in 'Internal vulnerabilities to external risks' in this part.

See 'Personnel security' of the 'Departmental security' chapter for instructions relating to employee/candidates suitability, criteria, recruitment, condition of employment, identifying positions, vetting and process requirements involving national security clearances.

Managing risk

The key messages for managing security risks are:

- managing security risk is everyone's business
- like any risk management, security risk management is part of day-to-day business and should become habitual.

Part of our risk management strategy is to decide on how much protection is needed. Use general risk analysis the protective security capability maturity model to assess current capability across a number of protective security dimensions.

Risk management

Risk is inherent in policing, and everyone at Police has a role to play in managing risks.

Police's approach to risk management is set out in our Risk Management Policy. The Policy sets out the rationale, rules, and principles that underpin our approach and defines clear accountabilities for managing risk.

Police has a suite of tools to help you manage risk and apply our policy - https://tenone.police.govt.nz/page/risk-management

For further guidance, contact the Chief Risk Officer, Assurance Group, PNHQ.

Seven step risk management process

The Police risk approach is based on an internationally recognised risk management standard. The approach can be applied to any Police decision requiring resources to be allocated or action to be taken.

See, 'Organisational Risk Approach (2nd Edition) - Police Risk Management Framework' at paragraph 2.3 and appendix 4 for a detailed explanation of the 7 step risk management process.

Security measures

A single security measure is never complete protection. This section will assist you to plan and apply a combination of all security measures to ensure an appropriate security standard.

Three lines of defence model

Applying the defence model to mitigate risk

There are three levels of defence for mitigating risk, spontaneous risk management with service delivery, formal risk management/assessment and assurance.

Examples and responsibilities for each level of defence include:

Spontaneous risk management with service delivery	Formal risk management / assessment	Assurance
Responsibility with every Police employee. Examples: - intuitive - TENR - Operational threat assessment - Planning searches and assessing risk and community impact (Part 5 - Carrying out search powers with or without warrant)	Responsibility with: - supervisors - managers. Examples: - internal control - TSU Risk Management Manual - STG risk management procedures	Responsibility with: - Assurance Group - Principal Adviser: Protective Security - Chief Information Security Officer. Examples: - audit - debriefing operations and investigations

Districts/PNHQ Groups protective security plan

Districts and PNHQ groups must develop a protective security plan to manage their security risks and implement security measures.

The protective security plan must include controls to address all aspects of protective security:

- Governance arrangements (see 'Protective security governance')
- Personnel security (see 'Personnel security' of the 'Departmental security' chapter)
- Information security (see the 'Information security' chapters and in particular 'Information security')
- Physical security (see 'Physical security' of the 'Departmental security' chapter)

See:

- 'Annex 1 - PSR Mandatory requirements' that must be implemented and maintained in protective security plans. **Note:** Some requirements applicable for the national protective security plan may not be applicable for a District, Group or Service Centre plan. For example, appointing a Chief Security Officer is a single national role.
- 'Protective Security Capability Maturity Model (CMM)' and 'Annex 2 - CMM categories' to assess your current capability to manage risk and ways in which your risk management capability can be lifted.

Risk mitigation and assurance measures

Districts/PNHQ groups must select protective security mitigation measures on the basis of their identifiable

risks.

When deciding what risk mitigation controls are required, districts/PNHQ groups should undertake a full security risk assessment in accordance with:

- AS/NZS ISO31000:2009 Risk Management - Principles and guidelines
- HB 1672006 Security Risk management
- https://tenone.police.govt.nz/page/risk-management.

Reviewing risk assessments

Risk assessments should be reviewed when:

- undertaking new functions or varying existing functions
- moving a function to a new environment (e.g. a new location or the current location is refurbished)
- identifying a new risk
- a change in the National Security Threat Level has been announced by Government that indicates a change to the level of an agency risk or threat.
- a major security incident occurs, to ensure the conditions that allowed the incident to evolve are not present at your location.

Roles and responsibilities

Chief Security officer

See 'Chief Security Officer' in the 'Governance section'.

Security and Privacy Reference Group (SPRG)

The Security and Privacy Reference Group's (SPRG's) roles and responsibilities include:

- developing a strong and sustainable security culture within Police
- adopt a risk management approach to cover all areas of protective security activity across Police
- reviewing Police protective security management policy and procedures regularly as part of senior management's approach to risk management and business planning
- ensuring the mandatory PSR are being met and ensuring relevant oversight is in place
- supporting the Principal Adviser: Protective Security and working with them as they develop, maintain, and oversee protective security policy and practices
- endorsing security risk management structures, assurance activities and resource allocation
- endorsing Police policies and protocols for personnel, information and physical security.

Principal Adviser: Protective Security

The Principal Adviser: Protective Security has specific responsibility for Police to maintain oversight of good protective security requirements across the organisation by:

- establishing liaison between the district representatives (District Operations Managers) and the Chief Information Security Officer at PNHQ
- developing a strong and sustainable security culture within Police
- developing Police policy, procedures and protocols that comply with the mandatory requirements of the PSR
- reviewing Police protective security management policy and procedures regularly as part of the organisation's approach to risk management and business planning
- reporting to senior management (SPRG) on compliance against the mandatory requirements and agreed risk mitigation plans
- determining specific roles and responsibilities for security across Police
- providing guidance to senior management on security matters
- establishing and maintaining agreements and protocols with Professional Conduct Group to ensure awareness of all security breaches; breaches are properly investigated and appropriate action taken; and records are maintained
- managing and reporting security incidents and breaches including enhancing policies and procedures to prevent reoccurrences
- promoting and implementing protective security policy
- providing oversight of Police protective security
- developing and maintaining a certification/audit process to enable Districts with reporting PSR compliance

- giving advice and guidance on sensitive, strategic and risk areas affecting the protective security of Police
- arranging and coordinating security clearances with the NZSIS and GCSB
- remaining up-to-date with information about potential weaknesses in defences, new threat sources and threat types
- advising on employee safety, station security and asset protection
- ensuring that good quality protective security equipment, applications and practices are selected and installed
- ensuring that when corrective measures are required, improvements are implemented and applied
- liaising with protective security specialists in the government sector in New Zealand and overseas about emerging protective security issues
- ensuring that Police complies with the requirements of the PSR
- verifying Police's PSR compliance annually to SPRG for the Commissioner's sign-off.

Manager: Risk and Assurance

Role and responsibilities include:

- adapting effective risk practices and standards, and developing a risk approach for Police that is understood, owned and used across the organisation to assist the achievement of Police outcomes
- leading the implementation of strategies and processes so that risk management is integral to business planning, decision-making and the full range of operational and business processes throughout New Zealand Police
- providing the Executive and independent Assurance and Risk Committee with effective monitoring and visibility on risk
- working with the Executive, managers and teams across the organisation to develop and embed a risk-aware culture in which the Executive, management and all staff understand and take responsibility for managing risk
- being a source of expertise and advice on risk management approaches, tools and techniques, and the management of risk.

District Commanders/Directors

All District Commanders and Directors share responsibility for securing their District's, Group's or Service Centre's information and assets.

Districts, Groups and Service Centres must:

- consider protective security risks within their strategic risk management programme (for example, all new buildings and subcontractor sites must be subject to a security risk assessment, and plans must exist with at least biennial review dates)
- have an assurance/audit process that reports compliance level to the Commissioner via the Principal Adviser: Protective Security using the 'protective security workbook'
- comply with the protective security requirements and have a quality assurance system in place
- apply the Protective Security Capability Model to gauge their level of compliance
- monitor and determine what additional security (of people, buildings and information systems) may

be required.

Districts, Groups and Service Centres should:

- have an accreditation process that signs off all aspects of physical, person and information security
- where appropriate have their own protective security local orders/instructions (must be aligned to national policy in the Police Manual
- have a protective security programme that assures all procedures and requirements are co-ordinated (this includes business continuity planning [BCP]) Note: This will enable them to report on PSR compliance
- monitor and audit this programme annually and send the security self assessment checklist to their respective Deputy Commissioner or Deputy Chief Executive
- identify a person or position (e.g. District Operations Manager in district or designated group security manager[s]) to implement and coordinate protective security requirements.

District Operations Managers and designated group security managers

District Operations Managers are usually their District's security practitioner. Designated group security managers assigned by their Director are their group's security practitioner for specified areas within the group. District Operations Managers and designated group security managers are to apply the PSR, understanding it provides pathways for successfully protecting people, information and assets.

District Operations Managers designated group security managers responsibilities include:

- developing a strong and sustainable security culture within their District
- developing district/group-specific policy and procedures that comply with the mandatory requirements of the PSR
- reviewing regularly district's/group's approach to risk management and business planning with protective security management policy, procedures, induction programmes (ensuring security awareness training is applied and documented) and employment contracts (ensuring security awareness training is applied/documented)
- reporting to District Commander and Principal Adviser: Protective Security on compliance against the mandatory requirements and agreed risk mitigation plans
- determining specific roles and responsibilities for security across their district
- establishing and maintaining agreements and protocols with District/PNHQ Police Professional Conduct Managers to ensure awareness of all security breaches; breaches are properly investigated and appropriate action taken; records are maintained; and the Principal Adviser: Protective Security is informed of all breaches
- providing guidance to their District Commander and Principal Adviser: Protective Security on security matters
- managing and reporting security incidents
- promoting and implementing protective security policy
- providing oversight of district/group protective security.

Risk Coordinators (one per district or other national work group)

Role and responsibilities include:

- being a local source of advice and leadership on Police's approach to risk management
- supporting District Commanders/Directors in the systematic identification of risks (including security related) and the coordinated management of identified risks.

Area Commanders

Area Commanders must follow their district's security programme and ensure all security policy functions and requirements are undertaken.

Area Commanders must limit access to classified information and protected assets to those who need to know and who have the appropriate security clearances. Limiting access includes making sure that no single person can control all aspects of a process or system.

Area Commanders should also limit access to other assets that need additional safeguarding for availability or integrity purposes, or because of their monetary value.

All Police employees

Police employees play an important role in helping NZ Police maintain personnel, physical and information security.

By observing Police security policies, employees assure not only continuity of service delivery, but also assure the government and the public that Police has appropriate, effective measures in place to protect New Zealand's people, information and assets.

Police employees must observe security policies with the understanding they provide pathways for successfully protecting people, information and assets.

Police employees' responsibilities include:

- familiarisation with, and abiding by, Police security policies and procedures of their role dealing with:
    - personal safety of employees and clients
    - preventing financial fraud or theft
    - safeguarding equipment or plant
    - classified documents
- knowing who is responsible for protective security within their District, workgroup or Service Centre
- knowing their first point of contact for any questions about protective security
- reporting any security incidents, that have or might occur, to their District Operations Manager or designated group security manager
- depending on their role, they may also need to gain and maintain a national security clearance and clearly understand your security obligations and responsibilities as a clearance holder.

The '**Need to know principle**' is fundamental to good security. The only employees who should receive classified information are those who are authorised to receive it and require it in order to perform their assigned duties, as part of Police business.

Do not distribute classified information because it is nice or convenient to know, or because of another person's status, position or level of access.

It is essential to adhere to the 'need to know' principle to help protect Police employees and classified material. This applies both within the Police and when dealing with people outside it.

The '**Need to access principle**' is similar to the above except that it applies to potential access, by providing the capability of obtaining information which the person does not have a need to know. It is relevant to determine who has access to such as keys or combinations of secure rooms or containers, or to secured folders or applications on ICT systems for particular programs.

Providing access to new employees

These points apply when giving employees access to information:

- Access will be appropriate to the employee's clearance level
- Explain during the employee's induction the consequences of non-compliance
- All security incidents must be reported and, where appropriate, investigated (see: 'Personnel security'), especially incidents that:
    - may constitute a criminal offence
    - involve compromise to protecting information
    - involve threats to the national interest
    - affect availability of critical assets and services
    - affect Police operations or could require revisions to operational standards.

Managers and supervisors

Managers and supervisors must:

- give employees and service providers under their control sufficient information and security awareness to ensure they are aware of and satisfy the PSR. **Note:** See 'Security awareness learning' in 'Personnel security' for further guidance on training that must be provided.
- ensure all service providers are vetted before being engaged with Police.

Contractors and service providers

Private contractors and other service providers employed by Police play an important role in helping Police maintain personnel, physical and information security.

Service providers' responsibilities include:

- being aware of the PSR and the security policies and procedures that apply to Police (particularly their obligations set out in their contractual terms and conditions)
- understanding the impact of Police security policies and procedures on the services provided (services such as information management, information and communications technology, facilities design and management, personnel recruitment, general security services)
- developing a positive working relationship with Police to promote open communication and add

value to the security environment through the prompt identification and resolution of issues.

Depending on the role, service providers may also need to gain and maintain a national security clearance (sponsored by Police) and clearly understand their security obligations and responsibilities as a clearance holder.

Executive Director: People Operations

People Operations in the Corporate Operations Group are responsible for recruitment and employees management policies and procedures.

The Executive Director: People Operations must ensure:

- compliance with 'Personnel security'
- employees, service providers, contractors and volunteers are vetted prior to accessing Police information systems
- job descriptions reflect the PSR
- contracts and agreements for employees and service providers include standard protective security terms and conditions (Note: Contracts and agreements are only entered into where the service provider's protective security capability and practices can at least match those of Police) as well as requirements to undergo PSR initial and subsequent security awareness refresher training.

Chief Information Officer (CIO)

The CIO must ensure organisational compliance with these instructions:

- 'Information security'
- 'Acceptable use of information and ICT'
- 'Information security roles and responsibilities'
- 'Information classification and protection'
- 'Working with information classified CONFIDENTIAL and above'
- any other related parts of the wider 'Information security' chapters.

Director: Infrastructure

Physical security involves the proper layout and design of facilities and using measures to delay and prevent unauthorised access to Police premises and assets. It also includes measures to detect attempted or actual breaches or unauthorised access, and activate an appropriate response. Physical security also provides measures to safeguard employees from violence or intimidation.

The Director: Infrastructure must:

-
consider physical protective security risks and conduct security risk of all new buildings and subcontractor sites

-
ensure compliance with 'Physical security' in the 'Departmental security' chapter.

Manager: Security and Emergency Planning

The Manager: Security and Emergency Planning in the Frontline Capability Group is also expected to work closely with the Principal Adviser: Protective Security to ensure good practice for protective security is maintained throughout Police.

Protective Security Capability Maturity Model (CMM)

The CMM provides assistance for Districts, groups and Service Centres to:

- assess their security maturity across a number of protective security dimensions and identify maturity levels that are appropriate to the security risks they face
- identify some of the ways in which maturity could be lifted.

Protective security CMM levels

The following table provides the base descriptions for the protective security CMM levels:

Informal	**You meet the PSR mandatory requirements in some areas** - You assign resources to security work reactively, based on who is available rather than on role responsibilities or competency levels. - Your understanding of security risks is poor and inconsistent across your organisation. - You perform some basic security practices well and usually take corrective action when problems are identified. However, you implement improvements reactively after incidents rather than proactively to prevent incidents. - You rely on the expertise and effort of individuals rather than institutional knowledge and security culture; the loss of key people would significantly impair your security capability and practice. - Your security information is held in silos, may be duplicated, and may be in incompatible formats. - You lack the tools needed to support security management.
Basic	**You meet the PSR mandatory requirements in most areas** - You recognise the importance of security; key leadership responsibilities are assigned and understood. - You understand and occasionally review security risks and requirements · Security policies are in place, though they may not yet be well understood or supported by documented procedures. - Good practice is more repeatable than at the informal level, and results are more consistent, at least in some business units. - You plan and operate at least basic protective security measures. However, you plan, apply, and review your practices inconsistently. - You manage key security information well (for example, personnel records, risk assessments, policies, audit reports). - Tools and technologies supporting security management may meet basic needs, but are not centrally planned or easily integrated.

Managed	**You meet all the PSR's mandatory requirements and follow most supporting guidance** - Your executive team and relevant governance bodies support security. - Effective and robust security governance and management structures are in place. - Security is recognised and managed across the organisation at a strategic level. Security leaders are fully empowered to make decisions. - People responsible for leading security have the skills and resources they need. - You review your risk assessment and risk management processes to see if they will meet future needs. - You monitor and adapt to the risk environment in a planned and consistent manner. - Resource allocation is efficient and aligns to strategic priorities and risks. - Security policies, standards, and processes are well defined, understood, consistently followed, and produce the outcomes you expect · You monitor, assess, and evaluate security metrics to identify trends and patterns and where improvements should be made. - Tools and technologies supporting security management are well managed and fit for purpose. - Effective processes ensure performance targets are met and processes are well supported by toolsets. - Information from multiple sources informs your decisions and planning. You accurately evaluate the information's relevance and reliability.
Enhanced	**Security risks are viewed and managed as strategic organisational challenges** - Day-to-day activity adapts in response to changes in the risk and threat environment. - You continuously develop the skills of your security people to ensure knowledge remains current and relevant to your needs, and supports role succession. - You have mechanisms in place to develop and test security improvements. - You set and apply evidence-based measures to ensure performance is assessed objectively. - Tools and technology enable collaboration across your organisation and support process efficiency. - An effective continuous improvement programme operates that addresses outcomes, people, processes, information, and toolsets. - Long-term forecasting and planning is well integrated, with business planning cycles to predict and prepare for changes in the security environment and resource needs. - Security management information is captured, analysed, enriched, and distributed via enterprise services in real-time when needed.

Nature of CMM

The nature of capability maturity models are such that not every District, workgroup or Service Centre needs to achieve the highest maturity level in each of the following categories outlined in Annex 2:

- leadership and culture
- planning, policies and protocols
- personal security
- information security
- physical security.

The current security maturity target for Police is ‘MANAGED’.

Some aspects of Police operating environments may require to be ‘ENHANCED’, however, unnecessarily strong security measures are expensive and can impede the delivery of Police services.

It is not necessary that all elements of a lower level are in place before rating at, or aiming for, a higher level. The ‘informal’ and ‘basic’ levels are typically characterised by a lack of good practice

Assuring protective security performance

Assurance and Risk Committee (ARC)

In relation to the risk framework and internal controls, the Commissioner's ARC:

- provides assurance that appropriate risk management processes and internal control procedures are in place and operating effectively
- reviews Executive risk reporting, and provides an independent view on the coverage of key risks facing Police and the adequacy of the risk mitigation steps proposed
- reviews compliance with relevant statutory and regulatory requirements
- oversees progress with major projects and any associated risks.

Risk assessment

All members of a District, workgroup or Service Centre leadership team are responsible for protecting and securing its people, critical services, operations, infrastructure, information and other assets.

Districts, workgroups and Service Centres must:

- maintain a quality assurance system that reflects the PSR
- maintain risk assessments to identify risks and mitigation strategies
- monitor and determine what additional protective security (of people, critical services, operations, resources, buildings and information systems, etc.) may be required.

Assurance performance

Districts, workgroups and Service Centres must conduct assessments to ascertain their progress on meeting the direction and intent of PSR.

Periodic reviews must be performed to ensure Districts, workgroups and Service Centres:

- have a current risk assessment in place that shows their risks and mitigations
- monitor and determine what additional protective security (of people, critical services, operations, reputation, resources, buildings and information systems) may be required to cover the residual risks.

Where Districts, workgroups or Service Centres identify high protective security risks that after evaluation they are unable to mitigate, they must advise the Director: Assurance at PNHQ to ensure the risk is raised at the national level and should either:

- contact the Principal Adviser: Protective Security for advice and assistance, or
- elevate the protective security risk through their District Commander or Director to Police's Chief Security Officer.

Taking these approaches can ensure proactive steps are taken to remedy the situation. **Note:** The originating District, workgroup or Service Centre may not be the only location to identify such a risk. Communicating with others may identify:

- the protective security risk needs to be viewed from a national perspective, or
- another District, workgroup or Service Centre may have previously dealt with a similar matter.

Via communication, related issues can be identified and ensure a coordinated response.

However, an audit must be performed if the Commissioner directs such a step be taken, or there is a significant protective security failure.

Other government agencies

This table shows other government agencies that have a role in maintaining security in government

Agency	Function
NZSIS	- Establishes employee and physical security standards for national security information. - Advises government organisations on security standards. - Undertake employee vetting for national security clearances on request. - Manages the PSR on behalf of the government.
GCSB	- National authority for information systems security.
National Cyber Policy Office	- Formulates and co-ordinates common minimum standards for cyber security nationally. - Recommends how security policy is applied.

Local protective security instructions and orders

Districts

Each district must:

- conduct a threat and risk assessment to determine whether the protective security application is adequate to mitigate the security risks.
-
establish and maintain a protective security programme.

Protective security measures are a combination of:

Measure	Action
Laws, orders, instructions and plans	Local security orders and processes should be reflective of the Official Information Act 1982, Privacy Act 2020, Health and Safety at Work Act 2015, Crimes Act 1961, Protective Security Requirements, etc.
Physical measures	Physical obstacles and barriers, designed and placed to protect access to specific security interests.
Employee protective security measures	Only people whose reliability and trustworthiness are not open to doubt are provided access to Police information. Individuals who are granted a national security clearance continue to remain reliable while they remain in a position requiring a security clearance.
Protective security education and training	Ensures all Police employees, irrespective of access, understand both the threat and their general responsibilities for countering it. Protective security training ensures those individuals with specific security responsibilities, as part of their normal employment, are properly trained in their security duties. All managers are responsible for ensuring employees are aware and trained in 'Personnel security'.
Continuous review	A system of regularly programmed surveys, inspections, reviews and checks to ensure all protective security measures are maintained consistent with the security plan.

Annex 1 - PSR Mandatory requirements

The Protective Security Requirements (PSR) outlines the Government's expectations for security governance and for personnel, physical and information security. It includes mandatory requirements that Police must achieve and maintain.

Security governance

Security governance includes:

Governance	Requirement
GOV 1 Establish and maintain the right governance	Establish and maintain a governance structure that ensures the successful leadership and oversight of protective security risk. Appoint members of the senior team as: - Chief Security Officer (CSO), responsible for your organisation's overall protective security policy and oversight of protective security practices. - Chief Information Security Officer (CISO), responsible for your organisation's information security.
GOV 2 Take a risk-based approach	Adopt a risk-management approach that covers every area of protective security across your organisation, in accordance with the New Zealand Standard ISO 31000:2018 Risk management -Guidelines. Develop and maintain security policies and plans that meet your organisation's specific business needs. Make sure you address security requirements in all areas: governance, information, personnel, and physical.
GOV 3 Prepare for business continuity	Maintain a business continuity management programme, so that your organisation's critical functions can continue to the fullest extent possible during a disruption. Ensure you plan for continuity of the resources that support your critical functions.
GOV 4 Build security awareness	Provide regular information, security awareness training, and support for everyone in your organisation, so they can meet the Protective Security Requirements and uphold your organisation's security policies.
GOV 5 Manage risks when working with others	Identify and manage the risks to your people, information, and assets before you begin working with others who may become part of your supply chain.
GOV 6 Manage security incidents	Make sure every security incident is identified, reported, responded to, investigated, and recovered from as quickly as possible. Ensure any appropriate corrective action is taken.
GOV 7 Be able to respond to increased threat levels	Develop plans and be prepared to implement heightened security levels in emergencies or situations where there is an increased threat to your people, information, or assets.
GOV 8 Assess your capability	Use an annual evidence-based assessment process to provide assurance that your organisation's security capability is fit for purpose. Provide an assurance report to Government through the Protective Security Requirements team if requested.

Personnel security

Personnel security includes:

Personnel security	Requirement
PERSEC 1 Recruit the right person	Ensure that all people working for your organisation (employees, contractors, and temporary staff) who access New Zealand Government information and assets: - have had their identity established - have the right to work in New Zealand - are suitable for having access - agree to comply with government policies, standards, protocols, and requirements that safeguard people, information, and assets from harm.
PERSEC 2 Ensure their ongoing suitability	Ensure the ongoing suitability of all people working for your organisation. This responsibility includes addressing any concerns that may affect the person's suitability for continued access to government information and assets.
PERSEC 3 Manage their departure	Manage people's departure to limit any risk to people, information and assets arising from people leaving your organisation. This responsibility includes ensuring that any access rights, security passes, and assets are returned, and that people understand their ongoing obligations.
PERSEC 4 Manage national security clearances	Ensure people have the appropriate level of national security clearance before they are granted access to CONFIDENTIAL, SECRET, and TOP SECRET information, assets or work locations. Manage the ongoing suitability of all national security clearance holders to hold a clearance and notify NZSIS of any changes regarding their clearance

Information security

Information security includes:

Information security	Requirement
INFOSEC 1 Understand what you need to protect	Identify the information and ICT systems that your organisation manages. Assess the security risks (threats and vulnerabilities) and the business impact of any security breaches.
INFOSEC 2 Design your information security	Consider information security early in the process of planning, selection, and design. Design security measures that address the risks your organisation faces and are consistent with your risk appetite. Your security measures must be in line with: - the New Zealand Government Security Classification System - the New Zealand Information Security Manual - any privacy, legal, and regulatory obligations that you operate under. Adopt an information security management framework that is appropriate to your risks.
INFOSEC 3 Validate your security measures	Confirm that your information security measures have been correctly implemented and are fit for purpose. Complete the certification and accreditation process to ensure your ICT systems have approval to operate.
INFOSEC 4 Keep your security up to date	Ensure that your information security remains fit for purpose by: - monitoring for security events and responding to them - keeping up to date with evolving threats and vulnerabilities maintaining appropriate access to your information.

Physical security

Physical security includes:

Physical security	Requirement
PHYSEC 1 Understand what you need to protect	Identify the people, information, and assets that your organisation needs to protect, and where they are. Assess the security risks (threats and vulnerabilities) and the business impact of loss or harm to people, information, or assets. Use your understanding to: - protect your people from threats of violence, and support them if they experience a harmful event - protect members of the public who interact with your organisation - put physical security measures in place to minimise or remove risks to your information assets.
PHYSEC 2 Design your physical security	Consider physical security early in the process of planning, selecting, designing, and modifying facilities. Design security measures that address the risks your organisation faces and are consistent with your risk appetite. Your security measures must be in line with relevant health and safety obligations.
PHYSEC 3 Validate your security measures	Confirm that your physical security measures have been correctly implemented and are fit for purpose. Complete the certification and accreditation process to ensure that security zones have approval to operate.
PHYSEC 4 Keep your security up to date	Ensure that you keep up to date with evolving threats and vulnerabilities and respond appropriately. Ensure that your physical security measures are maintained effectively so they remain fit for purpose

Annex 2 - CMM categories

Use each of the descriptors shown in the PSR Capability Maturity Model to guide how you rate your existing maturity and also where your district or PNHQ group needs to be in order to meet the 'MANAGED' level of maturity. Further information can be found in this guidance.

MANAGED Capability	**Risk-based, fit-for-purpose security measures are in place, understood, and consistently followed. Ongoing investment is required to sustain measures at this level**
Leadership and culture dimensions	
Executive commitment and oversight	- How your executive or board promote security as a business enabler
Management structure, roles, and responsibilities	- How you allocate and support human resources to achieve your security objectives.
Monitoring and assurance	- How you provide confidence that your protective security measures are effective, efficient, and proportionate for the risks
Culture and behaviours	- How your people demonstrate security behaviours and actions
Education and communications	- How you build security knowledge, awareness, skills, and keep your people informed about security
Planning, policies, and processes dimensions	
Strategy and planning	- Formulating your security plan and bringing it to life.
Policies, processes, and procedures	- Clearly defining your expectations and approaches for achieving security
Risk management	- How you identify, assess, and mitigate your potentials risks, opportunities, and adverse effects
Incident management	- Expecting the unexpected and being ready to manage it.
Security Domains	
Personnel security	- Knowing who you have working for you and ensuring they are, and remain, suitable.
Information security	- Showing critical awareness on how to protect information in all its forms
Physical security	- Providing a safe and secure physical environment for your people, information, and assets.