Overview of Protective Security Requirements

Protecting our people, information, and assets

PSR | Protective Security Requirements

Contents

About this overview....3

1. Core policies of the PSR 4

2. The framework for the PSR....5

3. Complying with the PSR.... 10

4. Security governance....12

5. Personnel security 19

6. Information security 23

7. Physical security....27

About this overview

This overview of Protective Security Requirements (the PSR) outlines the government's expectations for security governance and for personnel, information, and physical security.

The PSR is a policy framework that sets out what your organisation must do to manage security effectively. It also contains best practice guidance you should consider following. The PSR is suitable for both public and private sector organisations.

Effective security enables New Zealand organisations to work together securely in an environment of trust and confidence. Protecting your people, information, and assets helps your organisation to meet its strategic and operational objectives.

Who this overview is for

This overview is for:

- organisation heads
- security management staff
- contractors who provide protective security advice and services
- anyone involved with the security of New Zealand Government personnel, information, and physical assets.

What this overview covers

This overview covers the PSR's core policies and mandatory requirements. It gives information on:

- defining governance and management structures for security
- identifying security risks and needs for personnel, information, and physical security
- complying with the PSR's mandatory requirements

Core policies of the PSR

The PSR's core policies cover four key areas: security governance, personnel security, information security, and physical security.

All organisations should comply with the requirements in the core policy areas listed below.

Security governance
GOVSEC

GOV 1 — Establish and maintain the right governance

GOV 2 — Take a risk-based approach

GOV 3 — Prepare for business continuity

GOV 4 — Build security awareness

GOV 5 — Manage risks when working with others

GOV 6 — Manage security incidents

GOV 7 — Be able to respond to increased threat levels

GOV 8 — Assess your capability

Personnel security
PERSEC

PERSEC 1 — Recruit the right person

PERSEC 2 — Ensure their ongoing suitability

PERSEC 3 — Manage their departure

PERSEC 4 — Manage national security clearances

Physical security
PHYSEC

PHYSEC 1 — Understand what you need to protect

PHYSEC 2 — Design your physical security

PHYSEC 3 — Validate your security measures

PHYSEC 4 — Keep your security up to date

Information security
INFOSEC

INFOSEC 1 — Understand what you need to protect

INFOSEC 2 — Design your information security

INFOSEC 3 — Validate your security measures

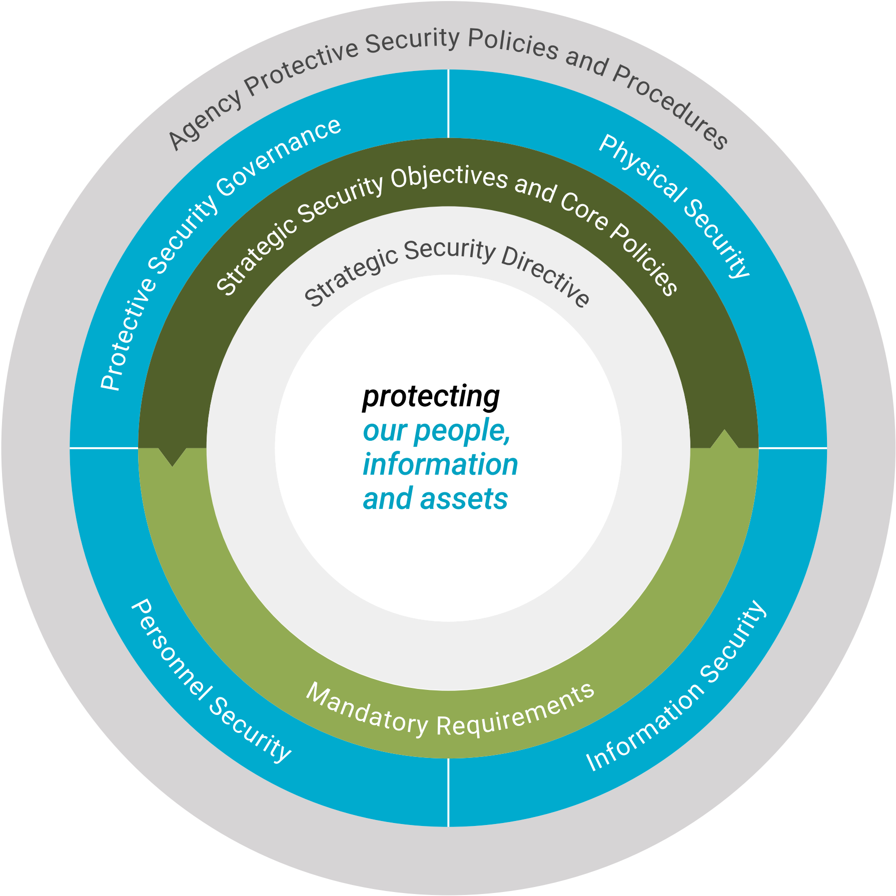
INFOSEC 4 — Keep your security up to date

The framework for the PSR

New Zealand's policy framework for protective security has four tiers and a hierarchical structure.

The four tiers support government and private sector organisations to implement protective security measures.

Protective Security Requirements framework



Agency Protective Security Policies and Procedures
Protective Security Governance
Physical Security
Personnel Security
Information Security
Strategic Security Objectives and Core Policies
Mandatory Requirements
Strategic Security Directive
protecting
our people,
information
and assets

Tier 1
Strategic security directive

The strategic security directive is the New Zealand Government's overarching security policy statement. It's the keystone of the PSR.

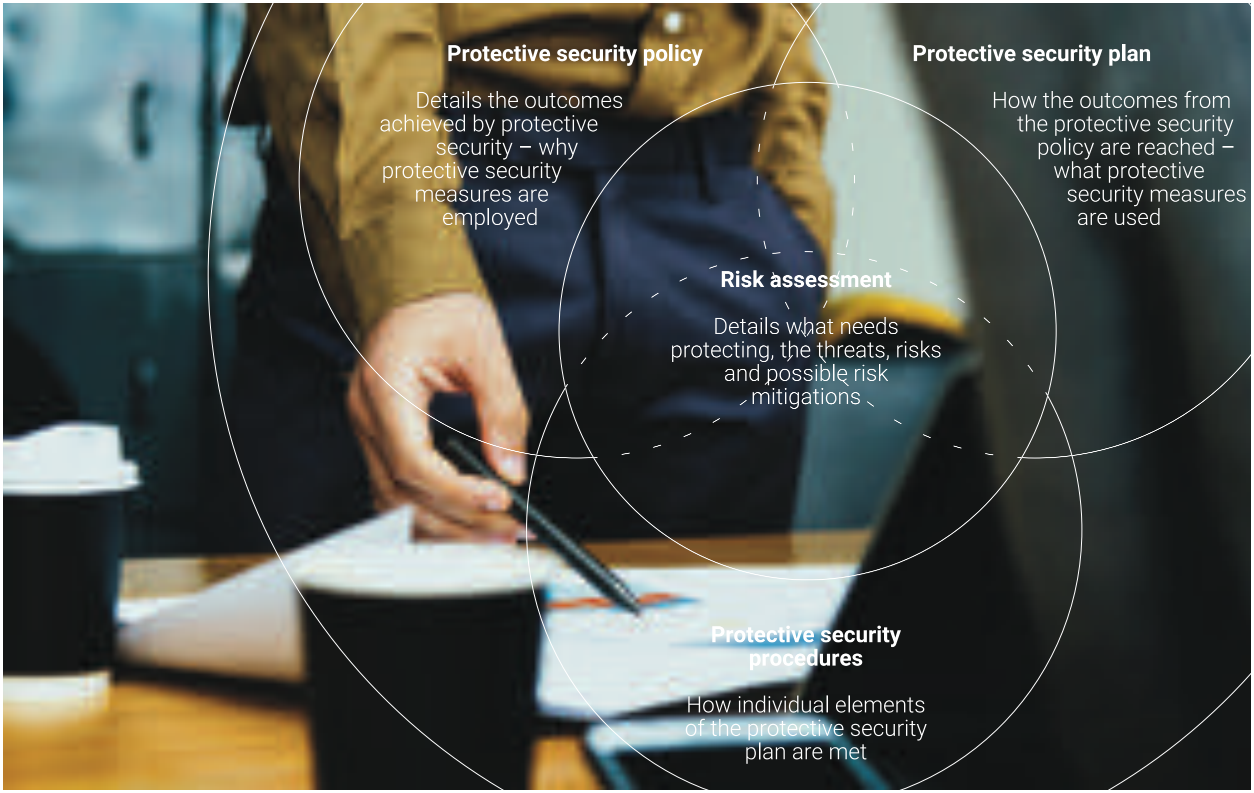
The directive articulates the government's requirement for protective security: *that it enables organisations to work together securely in an environment of trust and confidence.*

Tier 2
Core policies and mandatory requirements

Tier 2 contains the core security policies and mandatory requirements that government organisations must implement to ensure a consistent and controlled security environment throughout the public sector.

Once implemented, this tier enables government organisations to have more confidence in information-sharing practices and collaborative working arrangements.

The mandatory requirements span security governance, personnel security, information security, and physical security.



Protective security policy

Details the outcomes achieved by protective security – why protective security measures are employed

Protective security plan

How the outcomes from the protective security policy are reached – what protective security measures are used

Risk assessment

Details what needs protecting, the threats, risks and possible risk mitigations

Protective security procedures

How individual elements of the protective security plan are met

Tier 3
Protocols and best-practice guidance

Tier 3 provides detailed management protocols and guidance to support your organisation to implement mandatory requirements and establish best-practice security measures.

Key best-practice documents include:

- management protocols for conducting protective security activities to meet the mandatory requirements
- guidance for improving your security practices
- references to additional protective security and risk management resources and standards.

These documents standardise protective security practices across government to:

- enable information sharing
- support inter-organisation business
- help meet international obligations.

The New Zealand Government will continue to develop and refine protective security policy that promotes the most effective and efficient ways to securely deliver government business.

The policies and related protocols and requirements cover four areas: security governance; and personnel, information, and physical security.

Security governance

Good security governance is about conforming and performing.

'Conforming' means your organisation meets the PSR's mandatory requirements.

'Performing' means your organisation uses security measures to:

- contribute to your overall performance through the secure delivery of goods, services or programmes
- ensure the confidentiality, integrity and availability of your people, information and assets.

Applying governance principles

The PSR is based on the principles of public sector governance, including:

- **accountability** — being answerable for decisions and having meaningful mechanisms in place to ensure your organisation adheres to all applicable protective security requirements
- **transparency and openness** — having clear roles and responsibilities for protective security functions, and clear procedures for making decisions and exercising authority
- **efficiency** — ensuring the best use of limited resources to further the aims of the organisation, with a commitment to risk-based strategies for improvement
- **leadership** — achieving an organisation-wide commitment to good protective security performance through top-down leadership.

Personnel security

The people your organisation employs must be suitable for having access to official information and assets. They must meet standards for integrity, honesty and tolerance.

When necessary, your people must get a security clearance at the appropriate level.

Your organisation is responsible for managing your people throughout the employment lifecycle to prevent accidental or intentional security breaches.

Information security

The mandatory requirements for information security are based on the following elements:

- **confidentiality** — ensuring information is accessible only to those authorised to have access
- **integrity** — safeguarding the accuracy and completeness of information and processing methods
- **availability** — ensuring authorised users have access to information and associated assets when required.

Your organisation must also apply safeguards so that:

- information is protectively marked and labelled as required
- information in ICT systems is properly managed and protected through all phases of a system's life cycle.

Physical security

Your organisation must provide and maintain:

- a safe working environment for your people, contractors, clients and the public
- a secure physical environment.

Tier 4
Your organisation's policies, plans, and procedures

Your organisation must develop security policies, plans, and procedures that meet your business needs.

Your policies and procedures should:

- complement and support other operational procedures in your organisation
- include any risks your organisation creates that may affect other organisations
- consider any risks inherited from business partners.
- be at a standard that is equal to or higher than the PSR (not lower).

Protecting our people, information, and assets

Complying with the PSR

The PSR describes when your organisation needs to consider specific security measures to comply with mandatory requirements.

Identifying mandatory measures

A security measure with a 'must' or 'must not' compliance requirement is mandatory. You must implement or follow mandatory security measures unless you can demonstrate that a measure is not relevant in your context.

Identifying good-practice measures

A security measure with a 'should' or 'should not' requirement is considered good and recommended practice. Valid reasons for not implementing a security measure could exist, including:

- a measure is not relevant because the risk does not exist
- you're substituting a process or measure of equal strength.

Considering which measures to implement

Not using a security measure without due consideration may increase residual risk for your organisation. This residual risk needs to be agreed and acknowledged by your organisation head.

Pose the following questions before you choose not to implement a measure.

1. Is your organisation willing to accept additional risk? If so, what is the justification for your choice?
2. Have you considered any implications for all-of-government security? If so, what is the justification for your choice?

A formal auditable record of how you considered and decided which measures to adopt is required as part of the governance and assurance processes within your organisation.

Complying with legislation relating to security

The mandatory requirements and security measures are based on legislation relating to protective security and reflect government objectives.

When legislation requires your organisation to manage protective security in a way that is different to the PSR, that legislation takes precedence.

Some examples of legislation that might apply to some organisations are:

- Crimes Act 1961
- Criminal Discourses Act 2008
- Customs and Excise Act 2018
- Defence Act 1990
- Employment Relations Act 2000
- Health and Safety at Work Act 2015
- Income Tax Act 2007
- Official Information Act 1982
- Privacy Act 1993
- Public Finance Act 1989
- Public Records Act 2005
- State Sector Act 1988
- Summary Offences Act 1981.

Security governance

The PSR contains eight governance requirements which work together to ensure effective oversight and management of all security areas.

Establishing your governance structure

To implement protective security requirements, your organisation must clearly:

- identify your security governance structure
- define who is responsible for security governance.

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.

Develop a governance structure that enables you to effectively identify and manage security risks.

Your organisation head is responsible for reviewing and endorsing your proposed security risk management structures, assurance mechanisms, and resource allocations.

More information

Go to protectivesecurity.govt.nz and search for GOV005 to see the following page:

- Roles and responsibilities

Managing risks, and establishing policies and plans

The right risk-management approach will vary from organisation to organisation, but your process should be transparent and justifiable. Risk avoidance is not risk management.

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.

Your organisation's process for managing security risks should aim to:

- identify risks specific to your people, information and assets
- assess the likelihood and impact of risks occurring
- assess risks against vulnerabilities and the adequacy of existing safeguards
- specify your level of risk tolerance
- determine which protective measures are likely to reduce or eliminate risks
- identify and accept responsibility for residual risks
- implement security measures to reduce risks to acceptable levels.

Communicate about risk management to raise awareness

Common messages for managing security risks well are:

- everyone who works for your organisation is responsible for managing security risks (including contractors)
- risk management, including security risk management, is part of day-to-day business
- the process for managing security risks is logical, systematic, and part of your organisation's standard management processes
- changes in your organisation's threat environment should be continuously monitored and adjusted when necessary to maintain an acceptable level of risk and a good balance between operational needs and security.

Develop effective policies and plans

Your policies and plans for protective security should:

- detail the objectives, scope and approach to managing your security issues and risks
- be endorsed by your organisation's head
- identify security roles and responsibilities
- be reviewed when there are changes to your business or changes to your security risks
- be consistent with your security risk assessment findings
- explain the consequences for breaching policies or circumventing protective security measures
- be communicated regularly.

More information

Go to protectivesecurity.govt.nz and search for GOV003 to see the following page:

- Implementing a risk-based approach to protective security

Preparing for business continuity

Critical services and associated assets need to remain available to assure the health, safety, security and economic wellbeing of New Zealanders, and the effective functioning of government.

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.

A business continuity management (BCM) programme should be part of your organisation's overall approach to effective risk management.

BCM planning sets out the processes you should follow in the event of a disruption to business. A key risk for organisations is being unable to remain operational in the event of a crisis or other disruption.

Set up a robust programme

Carry out the following activities to ensure your BCM programme is effective.

In your governance arrangements, establish who oversees and takes responsibility for your BCM programme, and for developing and approving business continuity plans.

As part of your asset identification process, carry out impact analyses to identify and prioritise your organisation's critical services, assets, and information. Include any information exchanges with other organisations and external parties.

Develop plans, security measures, and arrangements to ensure your critical services and assets continue to be available. Include any other service or asset when warranted by a threat or risk assessment.

Monitor your organisation's overall level of preparedness for a disruptive event.

Ensure you continuously review, test, and audit your business continuity plans.

More information

Go to protectivesecurity.govt.nz and search for GOV012 to see the following page:

- Business continuity management

Building security awareness

To successfully deliver the PSR, everyone who works for your organisation needs to know and follow your security policies and processes.

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.

Educate everyone about your security requirements

To improve awareness of and compliance with your security measures, your organisation should:

- ensure people who have specific security duties receive appropriate and up-to-date training
- communicate your security polices to everyone who works for you, including contractors
- make sure your security policies easy to understand and access
- run an ongoing security awareness programme to regularly remind people of security responsibilities, issues, and concerns
- brief national security clearance holders on the conditions attached to their clearance level when they gain or renew a clearance, and when required in the clearance renewal cycle.

Uphold legislation for protecting official information

Provide everyone who works for you with guidance on the relevant sections of legislation covering the unauthorised disclosure of official information, including the:

- Official Information Act 1982 — sections 6, 9, 27 and 31
- Privacy Act 1993 — Information Privacy Principles, section 6
- Crimes Act 1961 — sections 78, 78A, 78B, 78C and 79
- Summary Offences Act 1981 — section 20A.

The combined effect of the Crimes Act 1961 and the Summary Offences Act 1981 is that the unauthorised disclosure of information held by the New Zealand Government is subject to the sanction of criminal law. Your people need to be aware of whether and how such legislation applies to their role.

More information

Go to protectivesecurity.govt.nz and search for GOV008 to see the following page:

- Building protective security awareness

Managing risks when working with others

The PSR applies as much to service providers and outsourced services as it does to your internal operations.

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.

When you outsource services or functions, your organisation should:

- apply personnel security procedures to private sector organisations and individuals who have access to New Zealand Government assets
- ensure government assets, including ICT systems, are safeguarded through specifying security requirements in contract terms and conditions, and visiting providers to assess compliance.

More information

Go to protectivesecurity.govt.nz and search for GOV019 to see the following page:

- Supply chain security

Managing security incidents

The purpose of a security investigation is to establish the cause and extent of an incident that has, or could have, compromised your organisation or the New Zealand Government.

The process of investigating and reporting security incidents also helps you to understand your vulnerabilities and reduce the risk of future incidents.

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.

Be fair and just when you investigate

A security investigation should protect both the interests of the New Zealand Government and the rights of affected individuals.

Your organisation must apply the principles of natural justice and procedural fairness to all security investigations.

Your procedures should give due regard to ensuring the integrity of any other current or future investigation by your organisation or that of another.

Report serious security incidents to the right authorities

If an incident is potentially serious, you must consult with the:

- New Zealand Police
- New Zealand Security Intelligence Service (NZSIS)
- Government Communications Security Bureau (GCSB) or the Government Chief Digital Officer (GCDO), or both.

More information

Go to protectivesecurity.govt.nz and search for GOV009 to see the following page:

- Reporting incidents and conducting security investigations

Responding to increased threat levels

Your organisation must be ready to respond to emergency and increased threat situations.

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.

Your plans for moving up to heightened security levels should integrate and coordinate with other emergency prevention and response plans. For example, plans for responding in case of a fire, bomb threat, hazardous chemical spill, power failure, evacuation, or civil defence emergency.

More information

Go to protectivesecurity.govt.nz and search for GOV007 to see the following page:

- Developing security alert levels

Assessing your security capability

An annual self-assessment helps your organisation to know if your security measures are right, and to improve security if you need to.

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.

Review your policies and plans every 2 years, or sooner if changes in the threat or operating environment make it necessary.

The assessment and reporting process aims to help your organisation check how well you're ensuring that:

- your people are safe
- your essential resources are retaining their confidentiality, integrity, and availability.

The process comprises internal self-assessment and reporting, and in some cases external reporting to lead security organisations.

More information

Go to protectivesecurity.govt.nz and search for SAR001 to see the following page:

- Self assessment and reporting

Personnel security

To protect government-held resources, your organisation must ensure that access to information and assets is only given to suitable people.

Your personnel security measures should start at the pre-employment stage and continue throughout the personnel lifecycle.

Taking a risk-based approach

Employ a risk-based approach to personnel security to reduce the risks of government resources being lost, damaged, or compromised.

A risk-based approach helps you make good security decisions, reduces unnecessary costs, and minimises disruption to your people and operations.

Use risk assessments to help you:

- identify the risks associated with each role
- adopt the right security measures for each stage of the personnel lifecycle.

Support your personnel security measures with effective line management, the correct application of the 'need-to-know' principle, access controls, and information security measures.

More information

Go to protectivesecurity.govt.nz and search for PER002 to see the following page:

- Management protocol for personnel security

Recruiting the right person

Personnel security helps your organisation to gauge the honesty, trustworthiness, and loyalty of people who might access government resources.

All people employed by the New Zealand Government may be subject to security vetting.

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.

Your organisation should:

- carry out the right pre-employment checks
- set the right expectations about security during induction.

More information

Go to protectivesecurity.govt.nz and search for PER007 to see the following page:

- Recruit the right person

Ensuring their ongoing suitability

Changes in personal circumstances, role requirements, or your organisation's risk profile can happen at any stage in the personnel lifecycle.

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.

Implement the following processes to ensure your people remain suitable for being employed and having access to your information and assets.

Report and respond to security incidents. Establish incident reporting and response procedures to help you manage security incidents. Aim to contain the effects, manage consequences, and recover quickly.

Carry out extra checks when security risks increase. Report significant changes in personal circumstances or suspicious activity. Report suspected criminal behaviour to the police.

Manage national security clearances. Provide education and briefings, report changes in personal circumstances, manage access and changes to clearance levels. Review clearances when required.

Make security everyone's responsibility. Raise awareness of your security practices and processes. Make it easy for your people to report suspicious behaviour.

Manage role changes. Carry out the right pre-employment checks before moving people into roles with higher risks.

More information

Go to protectivesecurity.govt.nz and search for PER009 to see the following page:

- Ensure their ongoing suitability

Managing their departure

When a person leaves your organisation, they retain their knowledge of your business operations, intellectual property, official information, and security vulnerabilities. Managing their departure well will reduce the risk of this knowledge being misused.

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.

Remove access and collect assets

Before a person leaves:

- remove their access to electronic resources, physical resources, and physical sites
- collect all identification cards and access passes, including any tools that allow them remote access to your information management systems
- make sure all assets are returned (take care with your intellectual property or official information).

Protect your organisation and others

To learn from the departure process and manage risks, you should also:

- conduct exit interviews
- assess and manage any risks you identify (for example, when someone leaves feeling unhappy)
- use a deed of confidentiality if the risk is high
- provide honest and accurate references.

More information

Go to protectivesecurity.govt.nz and search for PER010 to see the following page:

- Manage their departure

Managing national security clearances

The process of gaining a national security clearance ensures your people can be trusted to safeguard classified information, assets, or work locations. Once cleared, your organisation is responsible for managing their ongoing suitability to hold a clearance.

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.

Get a recommendation from the NZSIS first

Before your organisation grants a national security clearance, you must receive a security vetting recommendation from the NZSIS.

The NZSIS is responsible for the security vetting process and for making recommendations on security trustworthiness.

The security vetting process is intrusive. However, the NZSIS must conduct the process with care and sensitivity, and in line with government policy.

All vetting decisions are based on an assessment of the whole person, and the principles of natural justice and procedural fairness are followed throughout the process.

Even when your people have clearances, only grant access to protectively-marked resources when there is a legitimate need — do not give access based on convenience or someone's role in your organisation.

Know and meet your responsibilities for national security clearances

The following responsibilities are mandatory if you manage national security clearance holders. Your organisation must:

- identify, record, and review positions that require access to CONFIDENTIAL, SECRET, and TOP SECRET information, assets, or work locations
- check that the person has the right level of clearance before you grant them access
- ensure the ongoing suitability of all clearance holders to continue to hold a national security clearance.

Your organisation must also notify the NZSIS of any:

- decision to grant or decline a national security clearance
- decision resulting in a change to a national security clearance
- concerns that may affect the suitability of a person to obtain or maintain the appropriate level of clearance
- clearance holder who leaves your organisation or ends a contract with you.

More information

Go to protectivesecurity.govt.nz and search for PER026 to see the following page:

- Recruiting and managing national security clearance holders

Information security

The New Zealand Government collects and receives information to fulfil its functions and expects all those who hold or access this information to protect it.

Your information security measures should be based on your requirements for confidentiality, integrity, and availability of information.

What you need to do

Your organisation should develop, implement, and review security measures for protecting information from unauthorised use, accidental modification, loss or release. You do this through:

- establishing an information security culture
- implementing security measures that match your information's value, sensitivity and any protective marking
- adhering to legal requirements.

Definition of information asset

The term 'information assets' refers to any form of information, including:

- printed documents and papers
- electronic data
- the software or ICT systems and networks on which information is stored, processed or communicated
- the intellectual information (knowledge) acquired by individuals
- physical items from which information regarding design, components or use could be derived.

More information

Go to protectivesecurity.govt.nz and search for INF003 to see the following page:

- Management protocol for information security

Understanding what information you need to protect

To put right information security measures in place, you need to know what you have and how your organisation would be affected by any loss or harm.

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.

Take the following steps to comply with INFOSEC 1.

- Carry out an inventory of your information and ICT systems, including those that support business continuity and disaster recovery plans.
- Use the Business Impact Levels to assess the impact of your information being compromised. Find out where your organisation is vulnerable to security breaches, what threats you face, and how you would be affected.
- Include risks from your supply chain and from aggregated information (collections of information in electronic or hardcopy formats).
- Analyse your existing security measures to find out where you might need to improve.
- Classify and assign protective markings to information that requires it, so your people know how to handle the information and protect it.

More information

Go to protectivesecurity.govt.nz and search for INF023 to see the following page:

- Understand what information and ICT systems you need to protect

Designing your information security measures

Once you understand the risks to your organisation's information, you need to design fit-for-purpose security measures. These measures should be proportionate to your risks and in line with your risk appetite.

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.

Design your information security measures

Carry out the following actions to design fit-for-purpose security measures.

- Use multiple layers of security — 'security in depth' — to reduce the risks to your information.
- Know and address the points where your information could face critical risks.
- Create a framework for information security that balance security with costs and the impact on your operations.
- Include the security measures you design in your business continuity and disaster recovery plans.
- Comply with mandatory requirements for information, ICT systems, networks (including remote access), infrastructure, and applications.
- Get sign-off from your chief information security officer (CISO) or equivalent executive.

Implement your information security measures

Once your CISO agrees that the proposed security design will address your organisation's specific information security requirements, you need to:

- implement the agreed security and privacy measures, including policies, processes, and technical security measures
- work with your suppliers to ensure that they understand and can meet your security requirements
- account for the information risks involved in the ICT system development lifecycle
- test your systems during development and before acceptance.

Comply with relevant requirements

Your security measures must comply with any privacy, legal, and regulatory obligations that you operate under, and the requirements in the:

- *New Zealand Government Security Classification System*
- *New Zealand Information Security Manual.*

More information

Go to protectivesecurity.govt.nz and search for INF027 to see the following page:

- Design fit-for-purpose information security measures

Validating your security measures

You must validate the measures you implement to ensure they will work as expected.

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.

Your CISO is responsible for deciding whether your security measures will reduce your organisation's risks to an acceptable level. Your executive team can then have confidence in the measures, including how they'll be governed.

ICT systems must comply with the certification and accreditation process in the *New Zealand Information Security Manual*.

More information

Go to protectivesecurity.govt.nz and search for INF031 to see the following page:

- Validate your security measures

Keeping your security up to date

Threats, vulnerabilities and risks to your organisation's information will change as technology, business, and information needs change.

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.

To keep your information security up to date and comply with INFOSEC 4, carry out the following activities.

Analyse evolving threats and vulnerabilities. Monitor and observe so you can identify vulnerabilities and detect concerning events. Take proactive action to secure your systems, networks, configurations, and processes.

Keep your information security measures up to date. Maintain access control systems and protect ICT equipment. Ensure your business continuity and disaster recovery plans are tested when you adopt new or updated processes, systems, and capability.

Respond to information security incidents. Ensure you investigate and respond quickly, communicate with affected parties or relevant authorities without delay, and learn from incidents to improve security.

More information

Go to protectivesecurity.govt.nz and search for INF032 to see the following page:

- Operate and maintain to stay secure

Assessing your capability

Reviewing your measures will help you to improve, adapt, or change your information security when needed.

GOV8 — 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.

Review your policies and plans every 2 years, or sooner if changes in the threat or operating environment make it necessary.

A mixture of regular and periodic reviews along with an annual assessment will help you to know when change is necessary, and how well your measures are being implemented and followed.

You'll also know when information needs to be archived, destroyed, repurposed, or disposed of securely.

More information

Go to protectivesecurity.govt.nz and search for INF035 to see the following page:

- Review your security measures

Physical security

Every New Zealand Government organisation must have physical security measures in place to protect people, information, and assets.

Physical security is multi-faceted and complements your security measures in other areas.

Good physical security supports health and safety standards, and helps your organisation to operate more efficiently and effectively.

Take a risk-management approach to working out the right levels of physical protection for your organisation's people, information, and assets.

Understanding what you need to protect

Knowing where your vulnerabilities are is the first step towards robust physical security. You may need to protect:

- your people, information, and assets
- the public and customers
- cultural holdings.

Once you identify your risks, you must evaluate the likelihood and impact of each risk. Assessing your risks helps you understand where you need to take further action.

More information

Go to protectivesecurity.govt.nz and search for INF003 to see the following page:

- Management protocol for information security

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.

Under the Health and Safety at Work Act 2015, your organisation must:

- identify risks to your people and act to reduce them
- protect clients and the public from harm.

For your facilities, you need to consider how they'll be used, who will use them, and what will be stored in them.

Other areas to think about are:

- arrangements for people working away from the office
- co-location arrangements with other parties
- plans for new sites or buildings, and plans for alterations
- ICT equipment and information
- your supply chain.

More information

Go to protectivesecurity.govt.nz and search for PHY009 to see the following page:

- Understand what you need to protect

Designing physical security early

To reduce costs and improve effectiveness, consider your physical security measures early in any process for:

- planning new sites or buildings
- selecting new sites
- planning alterations to existing buildings.

You also need to assess physical security risks for people working away from the office, and for any shared facilities you use.

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.

Evaluate risks and prepare plans

You must evaluate physical security risks before you select sites. Then prepare site security plans which detail the security measures you need to mitigate the risks.

Comply with security zone requirements

Use the right security zones and their associated measures for protectively-marked information and assets. Security zones may also help to protect other valuable information and resources. Each zone comes with minimum requirements you must implement.

Apply good practice for physical security design

Good practice includes:

- following the 'Deter, Detect, Delay, Respond, Recover' model
- using multiple layers of security — 'security in depth'
- using NZSIS-approved security products when required
- addressing all points where your physical security could be breached
- knowing and complying with all relevant laws and standards
- applying 'Crime prevention through environmental design' (CPTED)
- adding physical security requirements to your business continuity and disaster recovery plans.

Get your physical security design accepted

Your chief security officer (CSO) must accept that the proposed security design is fit for purpose and will address your organisation's specific requirements.

Implement your physical security measures

Implementing your agreed physical security measures includes rolling out related policies and processes, and any technical measures you need.

Include physical security in your business dealings

Build physical security into your contracts, business relationships, and partnerships. Ensure everyone is aware of your physical security requirements and check for compliance.

Manage your planning and building processes

Make sure your physical security measures are implemented when there are new builds, refurbishments, or assets shifted from one workplace or area to another.

More information

Go to protectivesecurity.govt.nz and search for PHY013 to see the following page:

- Design physical security early in your processes

Validating your security measures

Your chief security officer is responsible for validating your measures. They need to decide whether your organisation's:

- physical security measures are well managed
- risks have been properly identified and mitigated
- physical security measures allow governance responsibilities to be met.

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.

Following the certification and accreditation processes for security zones will ensure your physical security measures provide the right levels of protection and are implemented correctly.

More information

Go to protectivesecurity.govt.nz and search for PHY038 to see the following page:

- Validate your physical security measures

Keeping your security up to date

Your threats and vulnerabilities are likely to change over time. New technology, processes, arrangements, and objectives can all mean that your physical security needs to change. You must be alert to changes and take action to keep your security up to date.

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.

Your people need to know about changes that affect them and any new policies you bring in. You should also encourage them to report any risks they encounter or are concerned about.

To stay on top of your threat environment:

- monitor systems, assets, and people
- observe events and processes so you can detect threats
- assess your measures regularly to see if changes are necessary
- analyse and report on risks
- apply and track fixes.

When security incidents happen, ensure you learn from what happened, including how well your organisation responds to and manages incidents.

More information

Go to protectivesecurity.govt.nz and search for PHY040 to see the following page:

- Operate and maintain to stay secure

Assessing your capability

Assess your physical security measures to find out what needs to be improved or changed to better protect your people, information, and assets.

GOV8 — 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.

Review your policies and plans every 2 years, or sooner if changes in the threat or operating environment make it necessary.

Use a combination of methods, such as monitoring and reporting, reviewing, and auditing to help you find out if:

- your physical security policies are being followed (including policies for retiring or destroying information and assets securely)
- your physical security controls are working as planned
- any new threats or business practices have emerged.

More information

Go to protectivesecurity.govt.nz and search for PHY041 to see the following page:

- Review your physical security measures regularly

New Zealand Government