PSR | Protective Security Requirements

Guide to personnel security for your organisation

December 2019

newzealand.govt.nz

Contents

Purpose of this guide

Use this guide to help your organisation put robust personnel security (PERSEC) measures in place to protect your people, information, and assets.

What you will find in this guide

This guide includes information about risk assessments and the four mandatory security requirements mandated government organisations must implement and comply with. Businesses and non-mandated organisations should consider adopting the same requirements and carrying out risk assessments as part of good personnel security practice.

Who this guide is for

This guide is primarily for chief security officers and security practitioners. It is also a useful reference for line managers and human resources staff.

The requirements in this guide apply to all people working for your organisation, including employees, contractors, and temporary staff.

For people who need a national security clearance, there are extra requirements, which this guide summarises. For more detailed information, see the following page on protectivesecurity.govt.nz:

→ Recruiting and managing national security clearance holders

If you are from a government organisation, this guide will help you to understand and comply with mandatory requirements for personnel security.

If you are in the private sector, this guide gives you advice on protecting your people, information, and assets. As good practice, we recommend you consider adopting the mandatory requirements for government organisations.

Why personnel security matters

Meeting the personnel security requirements and having good security measures in place allows your organisation to:

- reduce the risk of your information or assets being lost, damaged, or compromised
- have greater trust in people who have access to your organisation's information, assets and work locations.
- deliver services and operate more effectively.

Understand the risks people pose to your organisation

Although people are often said to be an organisation's greatest asset, they can also be a weakness.

Insider threats can come from your past or present employees, contractors, or business partners. They can misuse their inside knowledge or access to harm your people, customers, assets, or reputation.

Studies have found that most insiders who breach security had no malicious intent when they started their employment. Instead, they may become lax or 'go bad' as a reaction to later events.

Common ways an insider may breach security

Common insider acts can include:

- unauthorised disclosure of official, private, or proprietary information
- fraud or process corruption
- unauthorised access to ICT systems
- economic or industrial espionage
- theft, violence, or physical harm to others.

An 'insider threat', or 'insider', is any person who exploits, or intends to exploit, their legitimate access to an organisation's assets to harm the security of their organisation or New Zealand, either wittingly or unwittingly, through espionage, terrorism, unauthorised disclosure of information, or loss or degradation of a resource (or capability).

Common reasons an insider may breach security

An insider's motivation is often a combination of:

- revenge against an employer or colleagues
- uncertainty about their continued employment
- greed or financial gain
- political or religious ideology
- ego or notoriety
- coercion, manipulation, or exploitation from an external third party.

When insider cases are investigated, it's not uncommon to discover a pattern of past behaviour of security concern. In some cases, individuals will have come to the attention of previous managers.

Unintentional security breaches or near misses can result from:

- lack of awareness or attention to security practices
- being distracted
- being tailgated
- being fooled into unwittingly assisting a third party.

More information

→ Insider data collection study — UK Centre for the Protection of National Infrastructure

Take a risk-based approach

Implementing personnel security measures can be costly or disruptive. Your security measures must be considered in light of your organisation's security context, potential threats, and risk appetite.

A risk-based approach ensures your personnel security policies, practices, and investments are right for the risks your organisation faces.

Why you need a risk assessment process

A risk assessment process allows your organisation to:

- identify and prioritise any people-related risks
- identify appropriate countermeasures to reduce risks
- implement security measures in a cost-effective way that reflects the level of risk and complements existing practices
- highlight risks and proposed countermeasures to senior management
- monitor the effectiveness of your security measures.

Identifying risks associated with roles

Some roles within an organisation have specific risks that differ from other roles.

Your risk assessment process should enable you to identify the risks associated with each role in your organisation and the appropriate controls to apply at each stage of the personnel lifecycle.

In particular, your risk assessment should identify roles or groups of people who have greater potential to cause harm due to their access to:

- highly sensitive, valuable, or classified information
- large collections of information
- valuable assets.

More guidance from protectivesecurity.govt.nz

→ Risk assessment for personnel security

Create a security culture

Everyone in an organisation contributes to its culture. Organisational culture has a direct impact on security. Even with the best security processes and tools your organisation will still be at risk if people have a poor attitude toward security.

The following steps will help to create a positive and sustainable security culture that reduces the personnel security risks facing your organisation.

Get commitment from the top

The chief executive and senior team must be committed to effective security practices and procedures. They also need to model best practice throughout the organisation.

Build security awareness

People are much more likely to engage in your security culture if they understand the credible security risks that face your organisation. Increased awareness will help people understand that they have important security responsibilities and know what those responsibilities are.

Publish clear communications about security

Everyone needs access to clear policies and procedures that:

- explain the reasons for your organisation's security instructions
- outline legal, regulatory, and compliance requirements
- ensure people understand their responsibilities.

Support staff wellbeing

Provide people with access to support, such as a confidential employee assistance programme. Encourage them to report and deal with personal issues before they become a serious problem.

Manage concerning behaviour

Managers need tools and policies to identify, support, and manage people who display concerning behaviour to do with security, poor performance, or unacceptable conduct.

Avoid a blame culture

People who raise legitimate security concerns should be encouraged and seen as good corporate citizens rather than troublemakers.

Reporting emerging concerns or near misses should be treated as a way of helping colleagues who might be at risk, rather than getting them into trouble.

Mandatory personnel security (PERSEC) requirements

Government organisations must implement and comply with four mandatory personnel security requirements.

Together, these requirements help to ensure that access to information and assets is only given to suitable people. The four requirements are:

1. Recruit the right person
2. Ensure their ongoing suitability
3. Manage their departure
4. Manage national security clearances.

Private sector organisations should also consider adopting these requirements to safeguard their information and assets.

Each stage of a person's lifecycle with your organisation can require:

- baseline checks that apply to every person working for your organisation
- optional checks to apply when you identify an increased security risk
- mandatory checks that apply to national security clearance holders.

1. Recruit the right person

PERSEC1 — 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.

Carry out the right pre-employment checks

Carry out pre-employment checks on everyone you're considering employing. You should check the suitability of any employee (permanent, short-term, or contractor) who needs access to government information and assets before they're appointed to a role.

Do baseline checks for all roles

The mandatory baseline checks include:

- confirming their identity
- confirming their nationality

- confirming their right to work in New Zealand
- checking their references with their former employer
- conducting a criminal record check.

You can do your own pre-employment checks or get a third party, such as a recruitment agency, to do all or some of them for you.

Remember to get the applicant's consent first. Under the Privacy Act, you should get consent in writing before you or a third party gather information from referees or other sources. You should also tell the application how you will use the information that is gathered.

If you use a third party, make sure you're clear about what checks they'll do and to what standard. It's good practice to ask for:

- confirmation they've done the checks you requested
- copies of reference checks.

Confirm their identity

Government organisations must check and verify a candidate's identity at the pre-employment stage following guidelines for establishing identity from the Department of Internal Affairs (DIA). Businesses can also use these guidelines to improve their pre-employment checks.

To confirm someone's identity, ask to see an original document, such as their passport or birth certificate. Be mindful that:

- some people may have an alias (for example, a previous family name)
- some people may be known by other first names
- naming conventions differ between cultures.

If you find unexplained discrepancies in someone's identity documentation, ask your HR team for advice.

Useful resources from the DIA

→ Evidence of Identity Standard

→ Factsheets on checking evidence of identity documents

Confirm their nationality

It's important to confirm a person's nationality as it may affect which information they can access.

Confirm their right to work in New Zealand

If you're recruiting someone to work for your organisation in New Zealand, make sure they're either a New Zealand citizen or have the right kind of visa to work in New Zealand.

For people who aren't New Zealand citizens, check which visa they hold and whether the visa conditions allow them to do the job they're applying for.

If you're recruiting for an overseas post, check the applicant has the right to work in that country. Contact the relevant embassy to check work eligibility requirements.

Useful resources

→ Understand types of citizenship — govt.nz

→ Check your applicant's visa using VisaView — Immigration NZ

→ Get contact details for embassies — Ministry of Foreign Affairs and Trade.

Complete reference checks

How an applicant has performed and behaved in the past is a good indicator of their future performance and behaviour. Checking references thoroughly with previous employers or clients gives you an opportunity to validate information the candidate has given you.

Check that any referees are:

- recent (from their last employer)
- appropriate for the role (verify the person worked for the organisation, as evidenced in their CV)
- from a legitimate source (ask your HR team for help with this if needed)
- free from any conflicts of interest (such as being in a close personal relationship with the applicant).

It's good practice to take detailed notes from any verbal checks, such as phone conversations. File your notes for future reference.

If you have any concerns, consider carrying out some of the optional pre-employment checks as well.

Overseas referees can be harder to check but you should still make sure these are completed as thoroughly as possible.

Conduct a criminal record check

You need to carry out a criminal record check to help identify:

- criminal convictions that may make a person unsuitable for the role
- measures you might need in place to manage risk if you decide to recruit the person.

You must have the person’s consent in writing before you go ahead with a criminal record check.

If you’re concerned about the results of a criminal record check, some of the optional pre-employment checks might help you to get a clearer picture of the person’s trustworthiness and suitability.

Getting a New Zealand criminal record check

Criminal record checks are usually suitable for New Zealand citizens and residents who have been here for some time. To get a New Zealand criminal record check, apply to the Ministry of Justice.

Criminal record checks are not suitable for roles that come under the Vulnerable Children’s Act 2014 — for those roles, Police vetting is required.

Getting an overseas criminal record check

For overseas residents or recent migrants, consider whether you need to do an overseas criminal record check. Be aware that rules for requesting criminal records differ by country, and sometimes by state or territory too.

In some places, only the person the criminal record belongs to can apply for their record. In this situation, you could ask the person to apply for their record and give you an authenticated copy of it.

Useful resources

→ Apply for a criminal record check — Ministry of Justice

→ Recruit the right person (more information on Police vetting from protectivesecurity.govt.nz)

→ How to Obtain an Overseas Criminal Records Check: Quick Reference Guide — UK Centre for the Protection of National Infrastructure

→ Children's Act requirements — Safety checking — Orangi Tamariki.

Ministry of Justice criminal record check versus Police vetting

A Ministry of Justice criminal record check only covers convictions. Police vetting may also include information on any contact that the individual has had with the police including:

- active charges and warrants to arrest
- any interaction the individual had with the NZ Police, including family violence incidents and investigations that did not result in a conviction
- information subject to name suppression where the information is necessary for vetting purposes.

A Ministry of Justice criminal records check is currently free if you request one directly from them. Police vetting currently costs $8.50 plus GST.

Use optional checks to reduce risks you've identified

When you identify an increased security risk with a role or the nature of your organisation's work, additional checks could be necessary. For example, for an IT administrator who has broad access to your organisation's information, you may wish to take greater steps to ensure they are trustworthy.

The additional checks that you apply will depend on a range of factors including your organisation's security context and culture, and operating environment. Checks that may be appropriate include:

- psychometric tests
- qualifications check
- financial or credit checks
- Police vetting
- drug and alcohol testing.

You'll find useful information on how to carry out optional checks on the following page.

→ Recruit the right person

Be aware of extra risks with contractors

Giving a contractor access to your information and assets comes with the same security risks as for permanent employees, and some extra risks. To address the risks, follow the process and tips in our *Guide to hiring and managing contractors* and *Contractor lifecycle and checklist*, available from:

→ Managing contractors

Do mandatory checks for national security clearance holders

Mandatory checks for people who need a national security clearance are included in the vetting process, which is carried out by the New Zealand Security Intelligence Service (NZSIS).

Be cautious about employing a person for a role that requires a clearance before the vetting process

is complete to avoid potential employment issues.

More guidance from protectivesecurity.govt.nz

→ Recruiting and managing national security clearance holders

Be alert to warning signs

Factors that on their own, or together, may raise concerns about an applicant's integrity and suitability to work in your organisation, include:

- any current involvement with criminal activity
- withholding information about criminal convictions not covered by the Criminal Records (Clean Slate) Act 2004
- false statements in a CV or job application form
- false claims about qualifications or achievements
- unexplained gaps in the applicant's employment or residential history
- adverse character references
- conflicts of interest
- evasive behaviour when asked to verify information they have provided
- evasive behaviour or a refusal when asked to supply references or give consent for criminal record checks or credit checks.

Mitigate any concerns

If you have any concerns arising from the pre-employment checks, you should:

- assess how the risks are likely to affect the role the person may be employed for
- work out whether you can reduce the risks to an acceptable and manageable level.

Record what you discover

Remember to record all concerns that come up during pre-employment checks, risk assessments you carry out, and decisions you make to reduce or manage risks.

Create a risk management plan if necessary

If you employ a person with identified risks, work with them to create an individual risk management plan. Use the plan to support the person in their work, treat risks, and maintain your organisation's security.

Set the right expectations

When a new person joins your organisation, you must make sure they understand your security policies and practices and agree to follow them. The induction process provides a good opportunity to make them aware of your policies, procedures, and security expectations. The sooner you make new people aware of their responsibilities, the sooner they can contribute to keeping your information and assets secure.

For new people who are cleared to hold a national security clearance, you must also:

- brief them on any security matters that relate to their clearance
- establish a risk management plan if you received a qualified vetting recommendation.

Be aware that if you employ someone who is being vetted for a national security clearance but hasn't yet been given clearance, you run the risk of employment issues surfacing.

More guidance from protectivesecurity.govt.nz

→ Recruiting and managing national security clearance holders

2. Ensure their ongoing suitability

PERSEC2 — 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.

Effective pre-employment checks reduce the risk of threats to your people, information, and assets. However, people and their circumstances can change. Changes can happen over time or suddenly as a reaction to a particular event. You need to make sure that people remain suitable for having access to your information and assets.

Do minimum checks to ensure ongoing suitability

At a minimum you must:

- have a process for people to report security incidents and near misses
- investigate security incidents
- provide ongoing security awareness updates and training.

Report and respond to security incidents

Managing security incidents and investigations effectively is a basic part of good personnel security. When there is a security incident, good management helps your organisation to:

- contain the effects
- manage the consequences
- recover as quickly as possible
- learn from what happens.

At a minimum you must:

- establish a formal security incident reporting and response procedure
- report all personnel security incidents to the appropriate people in your organisation
- make everyone aware of their responsibilities and the procedure for reporting security incidents.

Good communication between managers and employees, along with clear security expectations and procedures makes it easy for people to raise concerns, and report changes and incidents.

Managers and co-workers are in the best position to notice changes in a person's behaviour or attitude. Encourage your people to report what they notice and make it easy for them to do so confidentially.

More guidance from protectivesecurity.govt.nz

→ Reporting incidents and conducting security investigations

Provide ongoing security awareness updates and training

Ongoing security education helps to keep your people, information, and assets safe and secure. It also enhances your security culture. When you increase your people's understanding of security practices and processes, you increase their 'care factor', and their 'do factor' — security becomes everyone's responsibility.

Carry out additional checks for higher risk roles

When you identify an increased security risk related to a role or the nature of your organisation's work, additional ongoing checks could be necessary. The checks that you apply will depend on a range of factors including your organisation's security context and culture, and operating environment.

Checks to consider

Additional checks you can consider to ensure ongoing suitability include:

- requiring people to report any significant change in personal circumstances (for example, a divorce, new partner, bankruptcy, foreign citizenship, or new and significant debt)
- requiring people to report any suspicious contacts
- encouraging people to report any suspicion of 'insider threat'
- carrying out an engagement survey to understand people's satisfaction and level of engagement
- briefing people on the risks related to international travel
- requiring regular police vetting
- carrying out regular financial or credit checks
- requiring drug and alcohol testing
- checking regularly for conflicts of interest
- obtaining copies of annual practising certificates.

Report significant change in personal circumstances

Significant changes in personal circumstances can arise from many different areas: relationships, finances, health, work issues, substance abuse, or new interests and contacts.

These changes can put people under pressure. They could act irrationally or inappropriately, or be vulnerable to exploitation by others.

Reporting significant changes in circumstances will help you to manage any risk of someone:

- breaching your security intentionally or unintentionally
- being coerced into breaching your security by an external party.

Your people should know which changes of circumstances they need to report and who they should report them to. If you're unsure which significant changes need to be reported, consult with your HR and security teams.

Report suspicious contacts or behaviour

Foreign officials, foreign intelligence services, and commercial, political, or issue-motivated groups can devote considerable energy to accessing information (for example, political, economic, scientific, technological, and military information).

Small pieces of information can all contribute to a valuable picture. Make sure your people understand that a seemingly innocent conversation or contact, such as an email, may be part of an intelligence gathering exercise. Contacts can be official (as part of a person's role) social, or incidental and can take place in a wide variety of contexts.

Your people should complete a contact report when an official or social contact appears suspicious, ongoing, unusual, or persistent (SOUP) in any respect. This contact could be with:

- embassy or foreign government officials within New Zealand
- foreign officials or nationals outside New Zealand, including trade or business representatives
- any individual or group, regardless of nationality, that seeks to obtain official or commercially sensitive information they do not have a valid 'need-to-know'.

Attempts to get information may involve techniques such as phishing or tailgating.

Brief people on the risks related to international travel

When your people travel overseas, they could be targeted by foreign intelligence services aiming to get access to classified information.

To protect your organisation and New Zealand's interests, consider providing advice or briefing your people on the risks and the security measures they need to take. When they return, debrief them to check for any contact that appears suspicious, ongoing, unusual, or persistent (SOUP).

Your employees, secondees, and contractors should:

- consult your chief security officer before travelling to check if a security briefing is necessary
- know what methods foreign agents may use to gather information
- understand how to protect your organisation's information and assets
- know what information they must protect
- know what information they can share and trade
- be aware of how to manage electronic equipment.

More guidance from protectivesecurity.govt.nz

→ Security advice for New Zealand Government officials travelling overseas on business

Carry out checks for national security clearance holders

For people who hold a national security clearance, in addition to your general ongoing suitability checks, you must:

- provide annual security awareness updates
- conduct security briefings
- ensure they report any change in their personal circumstances
- ensure they report any suspicious contacts
- manage any emergency access to classified material
- report changes to their security clearance level
- review their security clearances.

More guidance from protectivesecurity.govt.nz

→ Recruiting and managing national security clearance holders (webpages)

→ Guide to managing national security clearance holders (PDF for printing)

Manage role changes

It is common for people to enter an organisation in one role then move to another role with greater responsibilities and a higher risk profile. Not completing the appropriate checks for the new role because the person is 'known' to the organisation increases the risk of problems.

Before you confirm a person in a new role, make sure you complete all required pre-employment checks and/or ongoing suitability checks to the level required for the new role.

3. Manage their departure

PERSEC3 — 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.

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.

Carry out minimum departure activities

At a minimum you must:

- remove access rights
- collect security passes
- make sure assets are returned.

Consider additional departure activities

Additional ways you can manage risks at the departure stage include:

- conducting an exit interview
- signing deeds of confidentiality.

Conduct exit interviews

In addition to their broader function, exit interviews give you the opportunity to remind the departing person of their obligations to protect your organisation's information.

Exit interviews are also a good opportunity to allow people to:

- discuss their reasons for leaving, and their attitude to your organisation and people
- surrender any passes or access cards they hold.

Use a deed of confidentiality if the risk is high

A deed of confidentiality may be necessary to protect your organisation's proprietary information or intellectual property.

Carry out all departure activities for national security clearance holders

For people with a national security clearance you must carry out the minimum exit steps, *and*:

- conduct an exit interview
- cancel or transfer their clearance
- debrief them from any secure compartmented information briefings they hold
- notify the NZSIS.

Assess and manage risk

A person who leaves feeling unhappy is less likely to be loyal and may pose a greater risk. Managers should assess and manage any risk a departing person may present. Depending on the level of risk, managers may need to restrict access to information, assets, and work locations at an early stage of the departure process.

4. Manage national security clearances

PERSEC4 — 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.

Anyone who needs to access information, assets, or work locations marked CONFIDENTIAL, SECRET, or TOP SECRET must first be granted a national security clearance by your chief executive, or their delegate.

The level of clearance is based on the security classification of information, assets, or work locations that a person needs to access to fulfil their duties — not on rank, seniority, or status.

To manage national security clearances, your organisation must:

- identify, record, and review positions that require access to CONFIDENTIAL, SECRET, and TOP SECRET information, assets, or work locations
- get a recommendation from the NZSIS before granting a clearance
- 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 clearance.

Notify the NZSIS of decisions, concerns, and changes

Your organisation must also notify the NZSIS of any:

- decision resulting in a change to a 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.

*Tell the NZSIS whenever a clearance is:

- granted or declined
- upgraded or downgraded
- suspended or renewed
- transferred to or shared with another organisation
- extended
- cancelled.

More guidance from protectivesecurity.govt.nz

→ Recruiting and managing national security clearance holders

Evaluate how well you are doing

Adopt a ‘layered approach’ to ensure your organisation’s security systems and practices meet your current needs and evolve over time to match changes in your risk environment.

A layered approach means carrying out multiple review activities to inform improvements to your personnel security measures.

Activities that can support continual improvement include:

- learning from your incident reports
- completing annual self-assessments against the Protective Security Requirements (PSR)
- reviewing your personnel security risks every two years.

Learn from your incident reports

Information you gather on security incidents and during investigations may highlight the need to reassess your current practices or arrangements. Use what you learn to identify opportunities for improvement.

Complete annual self-assessments

Government organisations must complete an annual self-assessment against the PSR. This self-assessment is also recommended as good practice for private sector organisations.

Self-assessment enables your organisation to:

- evaluate the effectiveness of your protective security measures
- identify areas of non-compliance with the PSR and ensure they’re addressed
- identify action you can take to mitigate risks and educate your people about security
- improve your protective security policies and procedures.

Review your risks every two years

We recommend you review your personnel security risks every two years in line with the following standards available from Standards New Zealand (www.standards.govt.nz).

→ AS/NZS – ISO 31000:2018 Risk Management Guidelines

→ HB 167:2006 — Security Risk Management — Handbook