PSR | Protective Security Requirements

Maintaining your national security clearance

December 2019

newzealand.govt.nz

Contents

About this guide

This guide tells you about your responsibilities as a national security clearance holder, so you can meet them and stay suitable to hold a clearance.

You should also make sure you know and follow your own organisation's policies for clearance holders.

'Your organisation' means the organisation that is sponsoring your clearance. If you're working for more than one organisation and your clearance is shared between those organisations, make sure you find out which organisation you must report to and who your main contact is.

Why remaining suitable to hold a clearance is important

Holding a clearance may be an essential requirement for your role or a condition of your employment. It's in the best interests of you and your organisation that you remain suitable to hold a clearance.

Your responsibilities

To maintain your clearance, you must meet your responsibilities as a clearance holder.

Make sure you read and understand the following responsibilities, or get someone in your organisation to help you understand them.

1. Respect the ‘need-to-know’ principle

The ‘need-to-know principle’ is about only giving access or sharing classified information and resources with people who hold the right level of clearance and need the access to do their work.

If a person asks you for access but doesn’t have the right clearance level, you must say ‘no’. If a person has the right clearance level but doesn’t need access to the information to do their job, you must say ‘no’.

You must not share information, assets or work locations or give access to it just because someone:

- is in a position of authority
- wants to enter controlled areas because it is convenient

2. Report changes in your personal circumstances

Some changes in your personal circumstances can affect your suitability to hold a clearance because they:

- put you under stress
- affect your judgement
- cause conflicts of loyalty
- make it easier for people or groups to influence you or use your access.

You must report the following changes in circumstances to your organisation as soon as they happen. Your organisation can then assess the risks and act to reduce them if it needs to.

You start or end a close personal relationship

You need to report the start or end of a close personal relationship. A ‘close personal relationship’ is any relationship where you are close to a person — that closeness could be sexual, emotional, or financial.

When you are close to someone, you naturally want to protect them. But your desire to protect someone you are close to could put your organisation’s information and resources at risk. You can also be more open to pressure or influence in a close personal relationship.

Some relationships can cause a conflict of loyalty. For example, if you had a close relationship with a foreign citizen, it might cause a conflict between your loyalty to that relationship and your loyalty to New Zealand.

You visit a foreign country

You must report any visit to a foreign country, so that your organisation can assess the risks. Whether a country is a security risk depends on your role, the level of clearance you hold, and your organisation's responsibilities.

Any of your close relatives move to a foreign country

When a close relative moves to a foreign country, you must report it. 'Close relative' means anyone in your immediate family and any relatives or whanau you have regular contact with.

'Foreign country' includes any country outside New Zealand (except New Zealand protectorates such as Niue or the Cook Islands).

When a close relative or whanau member moves to a foreign country it can:

- cause you to have a conflict of loyalty
- give that country influence over you.

You plan to change your citizenship or country of residence

If you plan to become a citizen of another country, you must report it. Your organisation needs to be sure that you are loyal to New Zealand, and able to protect government information and resources.

If you plan to live in another country temporarily or permanently, you must report it. Living overseas could make you ineligible for a security clearance. Ask your organisation if you need more information about this reporting rule.

Your financial circumstances change

You need to report changes in your financial circumstances including when you:

- receive a large amount of money
- increase your debt level significantly (for example, taking out a mortgage)
- create new financial associations (for example, entering into business with someone or becoming a loan guarantor)
- experience financial hardship, such as bankruptcy or entering a No Asset Procedure.

Changes in your financial circumstances can put you under stress or bring you into contact with people who could influence you.

Your health or medical circumstances change

You must report changes to your health or medical care. Some health conditions and medical treatments can affect your ability to make good decisions about who to share information with. For example:

- prescription drugs can affect your judgement
- a serious medical condition could change your behaviour or cause financial difficulties.

You are involved in criminal activity, accidentally or deliberately

You must report any arrests, criminal charges, or serious traffic offences.

Even if you're accidentally or inadvertently caught up in criminal activity, you could be at risk of being

influenced or pressured by a criminal group. This may include your friends or flatmates doing something dodgy or illegal. You should report any of these events so that you and your organisation can manage any risks.

If you're deliberately involved, your organisation will reassess your suitability to hold a clearance.

You become involved with people or groups that may affect security

When you become involved with any people or groups (including societies or organisations) that could pose security risks, you must report your involvement.

Examples of groups that might pose security risks are:

- extreme political groups and extremist organisations
- special-interest or issue-motivated groups — especially ones that have an interest in projects you or your organisation are working on
- commercial organisations that could benefit from access to classified information.

Whether a person or group is a security risk depends on your role as a clearance holder and your organisation's role. If you're not sure about who to report, ask your organisation. It is better to ask than not report.

You are in a disciplinary process

If you're in a disciplinary process with your employer, you must report it. Your organisation will assess whether they can continue to rely on you as a clearance holder.

You have breached security or caused a security incident

You must report any security breaches or incidents that you're involved in — deliberately or accidentally. Your organisation needs to be sure that you're reliable and committed to the security of their information and resources.

You have other changes in personal circumstances that your organisation has told you to report

Along with the changes in personal circumstances listed above, your organisation (line manager or security team) might have other changes they need you to report. They'll tell you about any extra reporting rules when you are employed or granted a clearance. If you are not sure what else you need to report, ask your line manager or security team.

Complete a change of circumstance form

Use the following form to report a change of circumstance in your personal and professional life.

→ Change of circumstance form.

3. Report concerns about other people

Telling your organisation (line manager or security team) about concerning behaviours or incidents relating to people you work with lets them put in place ways to support that person and maintain the organisation's security culture.

You must report any significant changes in personal circumstances, concerning behaviours, or

security incidents involving people you work with as it could affect:

- their suitability to keep a clearance
- the security standards of your organisation.

To report a change in another person's circumstances, use the following form.

→ Change of circumstance form.

4. Report suspicious contacts and requests

You must report any suspicious contacts and requests to access your organisation's information and resources.

Some individuals or groups will try very hard to get access to government information. They could try to get access to:

- classified information and resources
- official information or intellectual property that is not usually available to the public.

If they did get access, New Zealand could be badly affected.

Be aware of the possible sources of security threats

The following groups or individuals might try to get access to your organisation's information and resources:

- foreign intelligence services
- foreign officials
- political groups
- criminal organisations
- commercial businesses
- issue-motivated groups or individuals.

Suspicious contacts can happen in many settings, not just through your work. The table below shows some of the many ways that suspicious contact could happen.

Work — examples	Personal life — examples
• Invitations to attend functions • Written correspondence • Visits to embassies, consulates • Involvement with trade missions or other international events • Overseas business trips • Business networking sites • Membership of institutes or professional associations • Unsolicited emails or phone calls • Introductions through a third party	• Sport and recreation activities • Overseas travel • Social interactions • Training or study (for example, language classes) • Social networking sites • Membership of international clubs or friendship societies • Unsolicited emails or phone calls • Introductions through a third party

Be alert to signs of suspicious or inappropriate contact

When you experience contact that seems suspicious, ongoing, unusual, or persistent (SOUP) in any way, you must report it. Although the first contact a suspicious person makes with you might seem harmless, their approach could be well planned, and take place over a long time. You might not be aware that you are a target.

Be alert to the following scenarios and warning signs and report any you experience.

- A contact asks for information about other people who work in your organisation.
- A contact asks to meet you away from your work environment.
- A contact encourages you to participate in a dodgy or illegal activity.
- A contact offers you hospitality or gifts.
- A contact pays you a lot of attention — flattering you or showing sexual interest.
- A contact is unusually interested in your work or personal activities or some specific aspect of your activities.
- You are introduced to another person who shows the same unusual level of interest.

Be especially wary of contact 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 from any country who tries to get access to official information for which they do not have a ‘need to know’.

Your organisation should have a contact reporting form that you can use. If not, use the following form.

→ Suspicious contact — reporting form.

5. Discuss overseas travel plans with your organisation

Before you book overseas travel (for personal and business reasons), discuss your travel plans with your organisation.

When you travel overseas, it’s harder to protect the classified resources that go with you — such as the information in your head.

Your organisation could have restrictions on the places you can visit, airlines you can use, and activities you can take part in. Check your organisation’s policy on overseas travel.

Before you finalise your travel plans, you must get formal permission from your organisation. You may also need a travel briefing to make you are aware of any risks.

More advice from protectivesecurity.govt.nz

You should also read the following advice before you travel overseas.

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

→ Travel Advice Electronic Devices.

6. Minimise risks from your social media use

As a clearance holder, you need to be very careful about what you post on social media, including work-related networks such as LinkedIn.

You must not post classified information. Or say that you have a national security clearance.

You must also avoid posting information about your work, unless it is for work purposes. Although posting unclassified information doesn't seem risky, it can have a big impact on security when it is combined with other information.

Post as little personal information about yourself as possible. Think about whether you should reveal:

- your employer
- your address
- your hobbies, likes, and interests
- your biometric information, such as full date of birth
- any compromising photos.

Remember, social media platforms are constantly evolving and may reveal more information about you than you expect (for example, your location). Also remember that you can't take things back once they are out on social media.

Sharing your work and personal information on social media could give foreign intelligence operatives an opportunity to recruit you or use you as an intelligence source.

Personal and work information can be used for 'phishing'. Phishing is when emails are tailored to your likes, hobbies, or background to get you to open an attachment or click a link that installs and executes malware.

7. Understand and comply with legislation and policy

To maintain your clearance, you must understand and comply with:

- the requirements of Crimes Act 1961
- your organisation's security policy
- the requirements in this guide.

Complying with the Crimes Act 1961 means you must not:

- use or allow access to official information in any way that puts the security or defence of New Zealand at risk
- use or disclose any official information to benefit yourself or others financially.

You can be jailed if you are convicted of a crime under the Crimes Act 1961.

Your organisation should help you understand their security policy. You need to make sure you follow their policy at all times.

If you need help to understand any of the rules in this guide, ask your organisation for help straight away.

8. Participate in regular reviews

The New Zealand Security Intelligence Service (NZSIS) will review your suitability to hold a clearance — usually every five years. A review could happen sooner if:

- specific risks were identified when you were granted your clearance
- your organisation is concerned about your conduct or other risk factors (for example, a significant change of circumstances).

In a review, the NZSIS check:

- that you have met any specific requirements
- if any changes mean that your clearance needs to be reassessed.

You should keep a file about any overseas travel, so you have the information ready for your next review.

Each year, your organisation might do an assessment to check whether you are still suitable for holding a clearance. If they do, you must take part in the assessment process and give honest answers to all questions.

9. Meet the requirements of any security risk management plan

If the vetting recommendation for your clearance included specific recommendations (‘qualifications’), your organisation should have agreed a security risk management plan with you.

You must meet the requirements of the security risk management plan to remain suitable to hold a clearance.

10. Meet your ongoing obligations when you leave

Your obligations as a clearance holder continue after your leave your current organisation and/or you no longer hold a clearance. You have a lifelong obligation to be discrete about your work and to protect classified information or resources.