PSR | Protective Security Requirements

Guide to managing national security clearance holders

July 2020

newzealand.govt.nz

Contents

Purpose of this guide

Use this guide to help your organisation put the appropriate personnel security measures in place for anyone who requires or holds a New Zealand national security clearance.

What you will find in this guide

This guide includes information about national security clearances, when they are required, and your responsibilities for managing them.

Who this guide is for

This guide is for chief security officers, security staff, and line managers responsible for managing people that require or hold national security clearances.

The requirements in this guide apply to all employees, contractors, and temporary staff who require a national security clearance.

Note: This guide uses the term ‘employment’ to cover any type of employment, including permanent and temporary employment or a contract arrangement.

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 official or important information and assets
- deliver services and operate more effectively.

National security clearances

Good personnel security regimes provide a level of assurance about the honesty, trustworthiness, and loyalty of people who have access to government resources.

Anyone who needs access to information, assets, or work locations classified as CONFIDENTIAL, SECRET, or TOP SECRET for their role must have a national security clearance (clearance).

The requirement for a clearance relates to a role not an individual. The clearance level a person needs is based on the highest classification of information, assets, or work locations they need to access to do their work. A clearance level is not based on rank, seniority, or status. Your organisation works out which duties require a person to have ongoing access to information, assets, or work locations classified CONFIDENTIAL or above, and therefore who needs to hold a clearance.

The government expects that the number of people who require clearances will be kept to a minimum.

You must check that a person has the right level of clearance before you grant them access to your organisation's CONFIDENTIAL, SECRET, or TOP SECRET information, assets, or work locations.

Who grants and manages clearances?

Your organisation's chief executive is responsible for granting clearances and managing risk. This function may be delegated (for example, to your chief security officer).

The New Zealand Security Intelligence Service (NZSIS) is responsible for the security vetting process and for making recommendations on whether to grant a clearance.

The 'need-to-know' principle

The fundamental rule of personnel security is that your organisation should base all access decisions on the need-to-know principle.

Before you grant access to classified information, assets, or work locations, you must:

- establish a legitimate need for access to carry out official duties
- ensure each person holds the appropriate level of clearance.

You must not grant access to someone because they are in a position of authority, wish to enter controlled areas, or because it is convenient.

Your organisation must ensure that all employees and contractors are aware of, understand, and use the need-to-know principle.

National security clearance levels

The four security clearance levels are:

- CONFIDENTIAL
- SECRET
- TOP SECRET

- TOP SECRET SPECIAL.

The levels of vetting needed for clearances are on an escalating scale. For each step up the scale, there is an increase in the:

- degree of intrusion into the candidate's privacy
- breadth and depth of inquiries
- time required to complete inquiries
- time required to carry out assessments and make recommendations
- degree of assurance of the candidate's trustworthiness, honesty, and loyalty to New Zealand.

More information

→ See 'Appendix 1: Security clearance levels'

Mandatory personnel security requirements

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.

Overview of your responsibilities

The following responsibilities are mandatory for organisations that manage national security clearance holders. To manage 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 New Zealand Security Intelligence Service (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.

Your organisation must also notify the NZSIS of any:

- decision to grant or decline a clearance
- 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.

Your organisation's responsibilities for managing clearance holders add specific requirements to the typical personnel security lifecycle.

Identify the need for a national security clearance

To determine the clearance each role requires, you need to work out what level of classified information, assets, or work locations each position needs regular and ongoing access to. Record what you find and review access requirements regularly.

Check eligibility for vetting

Before you request vetting for a national security clearance, you must check the person's eligibility and suitability. You need to:

- check their citizenship or visa status
- make sure their background in checkable
- check their suitability for holding a clearance

- apply your own eligibility criteria if appropriate.

Request vetting for a clearance

Your chief security officer is responsible for submitting vetting requests for clearances to the NZSIS using the Online Vetting Request (OVR) system.

Decide whether to grant a clearance

You must ensure a person holds the correct level of clearance before they are granted access to protectively marked information, assets, or work locations at CONFIDENTIAL, SECRET, or TOP SECRET level.

Set the right expectations

When you grant a clearance, make sure the clearance holder understands the responsibilities that come with holding a clearance and agrees to meet them.

Ensure their ongoing suitability

While effective pre-employment checks reduce the risk of threats to your people, information, and assets, 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, assets and work locations.

Manage their departure

When a clearance holder leaves, they retain their knowledge of your business operations, intellectual property, classified information, and security vulnerabilities. Managing their departure well will help to reduce the risk of this knowledge being misused.

Sponsoring a clearance holder from another organisation

Sometimes people in private sector organisations (for example, service providers you've outsourced work to) require clearances due to the information they need access to. In these cases, a government organisation must sponsor each clearance.

The sponsoring organisation must ensure that all the clearance management arrangements identified in this guide are followed as if the clearance holder were their own employee.

More information from protectivesecurity.govt.nz

→ Supply chain security

Identify the need for a national security clearance

People who need access to information, assets, or work locations classified as CONFIDENTIAL, SECRET, or TOP SECRET for their role, must have a national security clearance at the appropriate level.

If a person needs access to information, assets, or work locations marked IN CONFIDENCE, SENSITIVE, or RESTRICTED for their role, they *do not* need a clearance. However, the 'need-to-know' principle still applies. That means ensuring you restrict access to people who have an operational need and have passed your personnel security checks.

Working out who needs a clearance and at what level

To work out whether a person requires a clearance and at what level:

- analyse the duties of the position
- identify the highest level of classified information, assets, or work locations the person will need access to
- identify whether the person will have access to any collections of classified information (physical collections and collections of information in ICT systems)
- work out how long the person will need the clearance for (for example, is the role short-term or permanent?).

Remember to consult your security staff throughout this process.

Assessing access levels for classified information in ICT systems

Anyone who needs access to an ICT system that holds classified information marked CONFIDENTIAL or above must have a clearance that matches the highest protective marking of information held in the system.

You need to factor in:

- the value and sensitivity of collections of information
- any holdings of sensitive compartmented information (SCI)
- any information marked New Zealand Eyes Only (NZEO).

More guidance from protectivesecurity.govt.nz

You'll find more guidance on access levels for ICT systems on the following page.

→ Identify the need for a clearance

Understand limits to access for foreign nationals

You cannot allow foreign nationals to access:

- any information, assets, or work locations marked NZEO unless they have a NZEO waiver
- classified material released to New Zealand from another country unless that country has approved the access in writing.

These rules apply even if the person already has a national security clearance at the appropriate level. (Some exceptions apply in limited circumstances.)

Consider your options for short-term roles

If you need short-term or temporary cover for a role that requires a clearance, consider reassigning an existing clearance holder from within your organisation.

If you need a new clearance for a short-term role, talk to the NZSIS security vetting team about whether the person could be cleared in time to meet your needs.

Recruiting for positions that require national security clearances

When your organisation advertises a position that requires a clearance, it is good practice to:

- tell people they'll need to be vetted for a clearance
- include an outline of the eligibility criteria or a link to the eligibility self-check tool
- encourage people to get in touch with you if they're unsure about their eligibility or the vetting process.

Being up front and approachable about eligibility and what's involved with getting a clearance may mean you get fewer unsuitable applications for the role.

More information from protectivesecurity.govt.nz

→ Recruit the right person

Making a clearance a condition of employment

It is good practice to make getting and maintaining a clearance a condition of employment.

Ideally, you will have notified potential candidates of this condition in your advertising. If you haven't, tell your chosen candidate before you offer them employment and include the condition in their employment contract (or contract for services if they're a contractor or service provider). Apply this practice to internal candidates or secondment arrangements as well.

Check eligibility for vetting

Before you request vetting for a national security clearance, you must check the person's eligibility and suitability.

Your chief security officer is responsible for:

- making sure eligibility checks are done
- submitting vetting requests to the New Zealand Security Intelligence Service (NZSIS).

You can use our self-check tool to check the eligibility of your candidates. (LINK)

Check their citizenship or visa status

To be eligible for vetting, a person must be a New Zealand citizen or holder of a Residence class visa.

In rare circumstances, other candidates may be considered for security vetting. However, several steps are involved before you can request vetting.

Your chief executive or chief security officer must discuss the rare circumstances with the NZSIS first. If the NZSIS agrees, you can prepare and submit a business case for vetting (your chief executive must approve the business case before you submit it). Vetting can only go ahead if the NZSIS accepts the business case.

Make sure their background is checkable

Before you submit a vetting request, make sure each vetting candidate meets the minimum requirements for checkable background.

In most cases, a person's background must be checkable for the required period or back to the age of 18. In some situations, it can be hard to assess whether a person meets the minimum requirements. View the answers to common questions after the following table for guidance.

Clearance level	Background checking
CONFIDENTIAL	5 years
SECRET	10 years
TOP SECRET	10 years
TOP SECRET SPECIAL	15 years

What if the person is too young to have enough checkable background?

If a vetting candidate doesn't have enough checkable years because of their age, they're still eligible for vetting. The NZSIS vetting team may recommend that a clearance is granted for a shorter time.

For example, if the candidate is 20, they'll only be checked back to the age of 18 even if the checkable background requirement is 5 years. The recommendation from NZSIS vetting team may be that you only grant a clearance for 2 years.

What if a person has spent lots of time living overseas?

Time in Australia, Canada, the United Kingdom, and the USA is considered checkable. Time in other countries is generally not checkable. The NZSIS can let you know whether they consider the person's background checkable or not.

When candidates have worked overseas for a New Zealand Government organisation, their time in other countries can be checkable if that organisation gives assurance that they've managed the person in line with protective security requirements for clearance holders.

Contact the NZSIS vetting team for advice

What if you're recruiting the person from overseas?

If you're recruiting from overseas, the person will still need to meet the checkable background and eligibility requirements.

Check their suitability for holding a clearance

Before you request security vetting, you must have trust and confidence in the person and their ability to gain a favourable recommendation for a clearance.

To help you check their suitability, review your organisation's records (such as performance or disciplinary records). Look for any records that show the candidate may be unsuitable. For example, records of:

- dishonesty
- misconduct
- breaches of the Code of Conduct for the State Services.

You should also assess the person's strength of character and integrity. If you have doubts about whether you can trust them with access to classified information, assets, or work locations, do not submit a vetting request.

The NZSIS applies the following criteria and guidelines when they vet people for a security clearance.

→ Security assessment criteria and the adjudicative guidelines

Apply your own eligibility criteria if appropriate

If a risk assessment shows your organisation needs stricter criteria for deciding who you will request vetting for, apply those criteria during your eligibility checking process alongside the mandatory checks described in this section.

Request vetting for a clearance

A government organisation's chief security officer is responsible for submitting vetting requests for national security clearances to the New Zealand Security Intelligence Service (NZSIS) using the Online Vetting Request (OVR) system.

The OVR is a secure, automated web-based system. Only authorised people have access to the OVR.

The information candidates give in the vetting questionnaire can only be used for vetting purposes. Your organisation can check applications in the OVR to ensure the information is complete, but you can't access or use the information for any other purpose.

Before you submit a request for vetting, you need to be sure the person is eligible for vetting and likely to gain a favourable recommendation for a clearance.

Remember to wait until your organisation has received a vetting recommendation and granted a clearance before you allow any access to protectively marked information, assets, or work locations.

Requesting urgent vetting

Contact the NZSIS vetting team to discuss an urgent vetting request before submitting it. If the NZSIS agrees you can go ahead with a request, make sure you include:

- a brief description of the circumstances that make the vetting urgent
- when you need a response from the NZSIS by.

You should only request urgent vetting when it is critical to do so. Examples of such circumstances may include, but are not limited to, short-notice security vetting for:

- overseas postings or deployments
- involvement in security-related court cases
- attendance at courses for which a clearance is required.

Be conscious that prioritising one vetting request is likely to delay other requests.

Granting emergency access to classified material

In an emergency, your chief executive may grant a person who already holds a clearance access to information, assets, or work locations one level above their current clearance.

More information from protectivesecurity.govt.nz

→ Manage their security clearance

Decide whether to grant a clearance

After your organisation gets a vetting recommendation from the New Zealand Security Intelligence Service (NZSIS), you need to review it, decide whether to grant a national security clearance, and let the NZSIS know what you've decided.

You must also ensure vetting candidates know what their rights are.

Receiving a vetting recommendation

When the NZSIS finishes vetting your candidate for a national security clearance, they'll give their written recommendation to your chief security officer (CSO) or their delegate.

The NZSIS may recommend:

- a clearance at the level you requested
- a clearance at a lower level
- a clearance with specific recommendations ('qualifications') for managing it
- that you don't grant a clearance (that a clearance is not appropriate at any level).

Acting on a vetting recommendation

Remember that your organisation must not grant a clearance at a higher level than you requested vetting for.

If you grant a clearance, you are the sponsoring organisation for that clearance holder.

For a clearance at the level you requested

If the NZSIS recommends a clearance at the level you requested and you decide to grant the clearance, you must provide the clearance holder with:

- a briefing on their responsibilities to protect classified information, assets, and work locations
- requirements for reporting any change in circumstances or suspicious contacts
- details of your organisation's security awareness training programme.

For a clearance at a lower level

If the NZSIS has concerns that may lead to recommending a clearance at a lower level than you've requested, they may advise your CSO to withdraw the person's access to classified information, assets, or work locations above the level of the clearance recommended.

Your CSO should advise human resources of the outcome if the clearance was a condition of employment.

Your organisation can then confirm the employment condition is met, or decide whether you will withdraw the employment offer, redeploy the person, or terminate their employment.

Note: A vetting candidate has the right to complain if they're unhappy with a vetting recommendation or process. If a candidate complains, wait until the complaint process is finished before you take any action. Seek legal advice if needed.

With qualifications on the clearance

Your organisation should follow any specific recommendations ('qualifications') that the NZSIS makes for managing security risks associated with a vetting candidate.

If you decide you can accept and manage the risks, work with the clearance holder to put a security risk management plan in place to manage the risks.

For a clearance not to be granted

Your organisation should not grant a clearance when you receive an adverse recommendation from the NZSIS about the candidate. Contact the NZSIS vetting team for more information.

Granting a clearance to a foreign national

If your organisation decides to grant a clearance to a foreign national, it's a good idea to make gaining New Zealand citizenship by a certain date a condition of maintaining their clearance. This helps give assurance of their loyalty to New Zealand.

Advising the NZSIS of decisions and changes

Your organisation must tell the NZSIS about every decision and change you make to the status of a clearance. You must tell them whenever a clearance is:

- granted or declined
- downgraded or upgraded
- suspended or resumed
- transferred or leveraged (shared with another organisation)
- extended or cancelled.

Advising vetting candidates about their right to complain

Your organisation's CSO or delegate must tell vetting candidates about their right to complain. A vetting candidate has the right to complain to the Inspector-General of Intelligence and Security if they are unhappy with:

- how the NZSIS carried out the vetting process
- the recommendation the NZSIS made.

Complaints must be in writing and addressed to:
Inspector-General of Intelligence and Security
c/- The Registrar of the High Court of New Zealand
DX SX 11199
Wellington

More information

→ Complaints — Inspector-General of Intelligence and Security

Set the right expectations

If you're managing a clearance holder, you must communicate with them clearly to set the right expectations for their role.

Make sure the clearance holder understands your organisation's security policies and practices, and is aware of them when they change.

Your organisation must provide security awareness training and briefings to the clearance holder when their clearance is granted, and at least every 5 years. This is a condition of re-validating their clearance after 5 years. Briefings should detail the clearance holder's responsibilities for keeping information secure.

The clearance holder needs to understand and acknowledge their specific responsibilities as a national security clearance holder. Make sure they know that their continued employment is conditional on them maintaining their clearance.

Ways to ensure awareness and education include:

- establishing personnel security risk management plans
- providing additional briefings with the clearance holder relevant to their security level and role.

To help set expectations from the start, let clearance holders know that they will be evaluated regularly because their suitability to hold a clearance can change over time.

Establish a security risk management plan

When you receive a vetting recommendation from the New Zealand Security Intelligence Service (NZSIS) with specific recommendations ('qualifications') for security risk management, you must establish a security risk management plan with the clearance holder and provide a copy of the plan to the NZSIS.

Conduct security briefings as needed

Types of briefings you may give to people when they start, or for specific purposes, include:

- travel briefings and debriefings, and personal safety briefings when travelling overseas on official business or for personal reasons
- briefings and debriefings for accessing TOP SECRET material
- briefings and debriefings for accessing material with endorsement or compartmented markings or with codeword protection (Note: some of these briefings must be done by the NZSIS or Government Communications Security Bureau)
- briefings for high-risk destinations or locations
- briefings tailored for specific categories of employment (for example, the unique security issues for information technology (IT) staff, scientists, and others)
- briefings tailored to contractors, temporary employees, visitors, and families of staff
- briefings tailored to the person's particular security needs as part of an ongoing management plan
- risk management briefings in general, and protective security briefings in particular.

Ensure their ongoing suitability

Your organisation must consider personnel throughout a national security clearance holder's employment. While recruitment and departure processes offer clear opportunities to manage the risks associated with a clearance holder, the most challenging and critical stage of the personnel security lifecycle is managing the clearance holder throughout their employment.

Every clearance holder must report any:

- change in their personal circumstances
- suspicious contacts.

The clearance holder's organisation must:

- provide annual security awareness training
- conduct security briefings
- report and investigate security incidents
- manage emergency access to classified information, assets, and work locations
- report changes to the clearance holder's clearance level
- review the clearance holder's clearance.

Help them meet their responsibilities

You can help a clearance holder meet their responsibilities by providing security awareness updates and training. You should also handle any reports of changes in their personal circumstances or suspicious contacts.

Publish clear communications about security

Your organisation must ensure clearance holders have access to clear policies and procedures that:

- explain your security requirements
- outline all legal, regulatory, and compliance requirements
- ensure they understand their security responsibilities.

Provide yearly security awareness training and briefings

Every year, your organisation should provide security awareness training to clearance holders.

You should also conduct additional security briefings or debriefings with clearance holders when appropriate. For more information about security briefings, see 'Set the right expectations'.

Prepare for international travel

When clearance holders travel overseas for work or personal reasons, they risk being targeted by foreign intelligence services with the capability and intent to target New Zealand interests.

Clearance holders may be of interest to foreign intelligence services for several reasons, including New Zealand's:

- position on international issues and agreements such as trade
- strategic perspective and intentions on domestic policies
- innovations in science and technology
- agriculture, primary industries, and other sectors that attract significant interest from foreign investors
- defence and intelligence capabilities.

Remember that your clearance holders could be exposed to the same risks in New Zealand at conferences or while hosting international delegations.

Your organisation is responsible for managing any risks with international travel and ensuring that you give travel briefings for work-related trips. Brief clearance holders 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).

When to report international travel plans

If a clearance holder holds Sensitive Compartmented Information (SCI) briefings, they'll need additional approval to travel to specified countries.

For further advice contact: psr@protectivesecurity.govt.nz

More advice from protectivesecurity.govt.nz

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

Report changes in personal circumstances

Make sure your clearance holders report any significant change in their personal circumstances, so you can check whether it affects their trustworthiness and their ability to retain a clearance.

What 'significant change' means

The following changes in a clearance holder's circumstances are significant and must be reported to your organisation's chief security officer (CSO) or security team.

- Starting or ending a close personal relationship
- Living in or visiting foreign countries
- Relatives living in foreign countries of security significance
- Changes in citizenship or nationality
- Changes in financial circumstances (for example, significant increases in wealth or debt)
- Changes in health or medical circumstances
- Involvement in criminal activity
- Involvement with any individual, group, society, or organisation that may be of security concern
- Disciplinary procedures or security incidents
- Any other changes in circumstance that may be of concern to the clearance holder's organisation

More information from protectivesecurity.govt.nz

→ Ensure their ongoing suitability

Report significant changes to your chief security officer

Your clearance holders must immediately report any significant change in their personal circumstances to your chief security officer (CSO) and to their manager (when relevant). This reporting requirement helps to mitigate any possible conflicts of interest.

If your CSO is unsure whether a change in personal circumstances has significant implications for the holder's clearance, they should seek advice.

For advice, contact: psr@protectivesecurity.govt.nz

If other people in your organisation become aware of a significant change in a clearance holder's circumstances — a change that may affect their suitability to retain a clearance or uphold your organisation's security standards — they should report the change to your CSO.

Recognising and assessing a significant change in circumstance

When you know about a change in circumstance early on, it usually makes it easier to deal with the issue and prevent it from becoming a security concern. You can then reduce the risks to the clearance holder and your organisation.

What to do when your organisation is aware of a significant change

When a significant change in circumstance is identified or reported, your organisation must conduct a risk assessment based on whether the clearance holder can continue to hold a clearance. If you have doubts about continuing the clearance, your organisation should suspend or cancel it until the risk is mitigated or assessed as no longer present.

When your organisation must notify the NZSIS of a significant change

When a change in circumstance is considered significant or likely to present a risk to national security, your organisation must notify NZSIS vetting.

The NZSIS may consider it necessary for your organisation to submit a new vetting request for the clearance holder. If the NZSIS is satisfied that the clearance holder remains suitable to retain a clearance, then it will make a positive recommendation. The risk management advice may include specific measures your organisation must take.

Report suspicious contacts

A clearance holder must report any suspicious or inappropriate contacts or requests to access your organisation's classified information, assets or work locations to their CSO.

Instances of suspicious contacts or requests may include contact with:

- foreign officials and foreign nationals
- criminal groups or people
- other suspicious people.

Completing a suspicious contact report

A clearance holder should complete a contact report when an official or social contact has occurred that appears suspicious, ongoing, persistent, or unusual (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 that they do not have a valid ‘need-to-know’.

→ Contact reporting form

Assessing a suspicious contact report

Your organisation should assess all suspicious contact reports to work out whether you need to:

- collect contact reports from other concerned people, and assess those reports
- advise the NZSIS of contacts that may have national security implications
- do an internal investigation
- contact the NZ Police (see below).

Sometimes a clearance holder’s inappropriate contacts may be of a criminal or business nature that involves a conflict of interest or gives an unfair advantage. Your organisation should have a clear process to investigate these contacts and, if appropriate, notify appropriate authorities for further investigation (for example, NZ Police, Serious Fraud Office).

More information from protectivesecurity.govt.nz

→ Reporting incidents and conducting security investigations

Manage their security clearance

Managing a holder's security clearance includes monitoring any concerning behaviour, reporting and responding to security incidents involving them, managing their emergency access to information, assets, or work locations, and managing changes to their security clearance level.

You also need to understand what's involved with reviewing, extending, sharing (leveraging), or transferring a clearance.

Monitor concerning behaviour

If you're managing a clearance holder, you must monitor their behaviour for any concerns to do with security, poor performance, or unacceptable conduct. Monitoring also means watching for any signs that could suggest the person is unreliable or susceptible to pressure. Pay particular attention if the clearance holder:

- is under 20 years old (their character is still forming)
- is unwilling to talk about matters, but is clearly unhappy
- has few friends and appears to be alienated from their colleagues.

A sense of perspective is required when considering these factors. And remember to act within your normal 'duty of care' responsibilities as a manager.

If you discover a behavioural issue, you must use your organisation's tools and policies to identify, support, and manage the clearance holder through any resolution process.

Report and respond to security incidents

Effectively managing security incidents and investigations is a basic part of good security.

Your organisation must keep records of all:

- security infringements, including breaches of organisation policy and procedures that lead to a compromise of the national interest
- security breaches, such as an accidental or unintentional failure to observe the requirements for handling classified information or assets
- security violations, including a deliberate action that leads, or could lead, to a compromise of classified information, assets, or work locations.

Provide details of security breaches to the NZSIS

If you think a clearance holder has breached security, your chief security officer (CSO) needs to assess the situation and identify the response, which may include advising the New Zealand Security

Intelligence Service (NZSIS) or the Government Communications Security Bureau (GCSB).

What is a security breach?

Review for cause

A 'review for cause' is a review of a clearance holder, undertaken by the NZSIS, when your organisation identifies security concerns that could affect their suitability to retain a clearance.

Your organisation should initiate a review for cause in response to any security concerns raised about a clearance holder.

Security concerns would normally relate to significant changes in the clearance holder's:

- personal circumstances
- attitude
- behaviour.

Concerns about the clearance holder can come from:

- the clearance holder
- the clearance holder's colleagues or supervisor(s)
- any other person who reasonably believes the clearance holder's personal circumstances, attitudes, or behaviour has changed.

Suspend access if necessary

If your organisation is investigating a clearance holder because of a security violation, your CSO should suspend their access to classified information, assets, or work locations until the investigation (which may include a review for cause) is complete.

Revoke a clearance if necessary

Regardless of any recommendation from an NZSIS review for cause, your chief executive has the right to revoke a national security clearance if they consider the security concerns, breaches, or violations are too frequent or of a sufficiently serious nature.

More information from protectivesecurity.govt.nz

→ Reporting incidents and conducting security investigations

Manage emergency access

Sometimes an emergency may give rise to an urgent operational need for a clearance holder to access classified information, assets, or work locations above their clearance level. Your chief executive or their delegate can grant this. If the authority is delegated, it must be recorded in writing.

What 'emergency access' means

Emergency access means your organisation has confirmed an urgent and critical operational need for access to specific information, assets, or work locations *and* there is not enough time to complete vetting checks and grant a clearance at a higher level.

Emergency access must be:

- only to specified information, assets, or work locations required for the emergency
- only for the duration of the emergency
- governed by a very strict application of the need-to-know principle
- provided at no more than one level above a person's current clearance*
- supervised by a manager with a suitable clearance.

*For example, if a clearance holder's current clearance is CONFIDENTIAL, their manager (with a suitable clearance) may supervise them to view SECRET material while the emergency lasts.

Recording, briefing, and debriefing requirements

The manager must record that the emergency access has been granted and brief the clearance holder appropriately.

The clearance holder must acknowledge that their manager has briefed them before being granted access. Your organisation should record this acknowledgement in writing.

Your organisation must also debrief the clearance holder when the emergency ends.

Limits to using emergency access

You must not use emergency access to grant a clearance holder access:

- for administrative or management purposes (such as helping them gain a position)
- when they are on reassigned duties while waiting for a security vetting recommendation (including a reclassification)
- to classified information, assets, or work locations that carry an endorsement or compartmented marking.

You must not grant emergency access to information, assets, or work locations marked CONFIDENTIAL or higher to anyone who does not hold a clearance.

Manage changes to their security clearance level

Sometimes a clearance holder's clearance level or status will change. Your organisation's CSO must tell the NZSIS whenever a clearance is:

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

Review clearances after 5 years

A national security clearance expires after 5 years (or sooner if your organisation has granted it for a shorter term) or when the clearance holder leaves their employment.

The clearance holder's manager is responsible for managing the process to ensure the clearance

continues, even if the clearance level changes.

Renewing a clearance

To renew a clearance, your CSO must first assess the clearance holder's ongoing suitability to hold a clearance. If the assessment result is positive, the CSO can submit a security vetting request to the NZSIS and they review the clearance.

Your CSO must have trust and confidence in the clearance holder's ability to gain a favourable recommendation from the NZSIS before they submit a security vetting request. To make such an assessment, your CSO must exercise their own judgement and view all information available to them objectively.

Your organisation should initiate a renewal of a clearance by the NZSIS early enough to maintain continuity of the clearance unless the person:

- is no longer in a position requiring a clearance, or
- has left New Zealand Government employment.

Extend a clearance

Your organisation may extend a clearance for up to 6 months at a time, up to a total of 12 months.

Example scenarios

The renewal process won't be complete before the clearance expires
1: Your clearance holder is in the process of getting their clearance renewed, but it doesn't look like the renewal will come through before the clearance expires, so you extend the clearance for 6 months.

2: Your clearance holder is deployed overseas so they can't complete their renewal forms. They're expected to return in 6 months, so you extend the clearance for 6 months. After 5 months, you realise the clearance holder won't be returning soon and still can't fill in their forms. You then extend their clearance for a further 6 months.

This clearance can't be extended again because it has reached its maximum extension time of 12 months.

The clearance expires before the end of a contract
A clearance is due to expire but the clearance holder's contract runs for 3 weeks beyond the expiry date. The clearance holder doesn't need a clearance after their contract ends, so instead of renewing the clearance, you extend it for 1 month.

You want to extend a clearance for a second time
Your clearance holder has their clearance extended for 1 month by their sponsoring organisation. Later on, the sponsoring organisation extends the clearance for another 6 months. These two extensions add up to 7 months, so the organisation has 5 months left for any further extension(s) out of the 12-month total.

Rules to remember

Your organisation can only grant an extension before a clearance expires and if there are no qualifications on the clearance.

You must complete your own due diligence to ensure the clearance holder is suitable for having their clearance extended.

You must continue to manage the clearance holder throughout the duration of the extension.

If the clearance is shared with another organisation (leveraged), you must review the sharing arrangement before you extend the clearance. Once a clearance has been extended, you must notify the other organisation.

Transfer a clearance

Your organisation might be able to transfer a clearance from a sponsoring organisation to yours. To do this, the clearance needed for the role the person is moving to must be at the same or lower level than the clearance the person already holds.

Government organisations can't grant a clearance at a higher level without first receiving a vetting recommendation from the NZSIS.

For more about transferring a clearance, go to: Manage their departure

Share (leverage) a clearance

If your organisation is planning to work with, or second, a clearance holder sponsored by another organisation, you may be able to use that clearance instead of getting a new one.

This situation may arise when a clearance holder's time is shared between organisations.

Both organisations need to consider whether the risks are acceptable before agreeing to a sharing arrangement.

Your joint responsibilities

If you agree to share a clearance, both organisations must:

- accept responsibility for sharing security concerns about the person
- agree on how you'll manage the clearance and what you'll each be responsible for
- inform each other about any changes in the clearance holder's circumstances you become aware of
- ensure the clearance holder gets appropriate security briefings.

Sponsoring organisation's responsibilities

- Get permission from the clearance holder before you share their personal information with the other organisation.
- If the original vetting recommendation for the clearance holder was routine, let the other organisation know that.
- If the original vetting recommendation was routine but came with information, qualifications, limitations, or adverse findings, share the original vetting recommendation with the other organisation.
- If you have any risk management plans in place for the clearance holder, share those plans with the other organisation.
- Notify NZSIS vetting that you are going to share a clearance and tell them who you'll be sharing it with.
- If you cancel or suspend a clearance, you must also suspend or cancel the sharing arrangement.

- If a clearance expires, you must cancel the sharing arrangement.
- If you downgrade a clearance, you must notify the other organisation.
- If you transfer the clearance to another organisation, the new sponsoring organisation needs to review and confirm the sharing arrangement is still acceptable to be in place.

Managing sharing arrangements — example scenarios

A clearance holder has contracts with different organisations

A clearance holder has two contracts at the same time with different organisations and requires a clearance for each job.

The clearance holder works 1 day a week at Organisation A and 4 days a week at Organisation B.

The two organisations agree that Organisation B should be the sponsoring organisation and Organisation A will share the clearance for the 1 day a week they have the clearance holder working with them. Organisation A knows to let Organisation B know of any change in circumstance during the contract.

A clearance holder is going on a short-term secondment

Organisation A sponsors the clearance holder and agrees to a short-term secondment to Organisation B. Both organisations agree to share the clearance for the duration of the secondment.

When the secondment ends, Organisation A cancels the sharing arrangement.

When the person has a current clearance from another country

If you want to work with someone with a security clearance from Australia, Canada, the United Kingdom, or the USA, get in touch with the NZSIS security vetting team to discuss the situation.

Upgrade to a higher clearance level when necessary

If the tasks or duties of a job change to the extent that a clearance holder needs to have access to information, assets, or work locations classified at a higher level than their current clearance, they must undergo security vetting at that higher level.

Your organisation will need to:

- ensure that the holder is eligible to hold a clearance at the higher level
- request security vetting from the NZSIS
- have the holder’s higher clearance level granted by your chief executive once a recommendation is received from the NZSIS
- brief the holder on any new obligations associated with their higher clearance level
- agree a plan for managing concerns or requirements in the NZSIS’s vetting recommendation.

Downgrade to a lower clearance level

A clearance holder may move to a new role that requires a lower level of clearance. This could be a permanent or temporary move. Alternatively, an organisation may decide that a person should have a lower clearance level. In these cases, a manager needs to confirm whether the lower security

clearance level will affect the clearance holder's employment agreement and how. Get HR or legal advice if you need it.

Later on, if you need the clearance holder to carry out duties at a higher clearance level, you can allow them to as long as:

- the initial vetting recommendation was at that higher level
- you are managing their clearance appropriately and there are no security concerns.

Withdraw access when the clearance is not granted, or until any review or appeal process is completed

See the following sections for more information on withdrawing access or handling review or appeal processes correctly.

Manage their departure

Maintaining your national security clearance

Procedural fairness

Evaluating your personnel security

Manage their departure

When a clearance holder leaves, they retain their knowledge of your organisation's business operations, intellectual property, classified information, and security vulnerabilities. Managing their departure well will help to reduce the risk of this knowledge being misused.

As well as the minimum requirements for an employee, when a clearance holder leaves an organisation, their manager must:

- remind them of their ongoing obligations
- transfer or cancel their security clearance
- notify the NZSIS.

An appropriately authorised person may have to:

- debrief the clearance holder from any access to SCI
- conduct an exit appraisal with the holder
- maintain post-separation contact with the departed clearance holder.

Remind them of their ongoing obligations

The clearance holder's manager must remind the holder of:

- the need for their continued discretion after they leave the organisation
- their lifelong obligation to protect classified information, assets, and work locations.

It is good practice to obtain the clearance holder's written acknowledgement of these obligations.

Transfer their security clearance

If the clearance holder is transferring directly to another government organisation, their clearance may transfer with them. In general, one organisation should recognise a security clearance granted by another organisation as long as the correct transfer process has been followed.

Accepting a clearance transfer

The chief executive of the new organisation may accept a transfer of a security clearance from another organisation. This action will happen immediately, provided the following conditions are met:

- the original clearance is less than 5 years old (however, if the original clearance is less than 12 months from its expiry date at the time of transfer, the new organisation should immediately begin the process to renew the clearance)
- there is a requirement to access classified information, assets, or work locations in the new role
- the transferred clearance is at the same level or at a lower level than the clearance originally recommended by the NZSIS
- the clearance holder moves directly from one government organisation to another without an

intervening period with no security oversight (for example, overseas residence or extensive travel)

- your chief executive obtains from the clearance holder's former organisation:
    - the vetting recommendation from the NZSIS (this may have important security risk management advice)
    - written assurance of the clearance holder's continuing suitability to hold a clearance
    - notification of any relevant changes in the clearance holder's personal circumstance that happened after they were vetted.

Signing a confidentiality agreement or post-separation contract

Your organisation may need the clearance holder to sign a confidentiality agreement as part of their transfer. This action is to protect any classified information, assets, and work locations they may discuss as part of their new role. They may also need to sign a post-separation contract with your organisation.

Managing briefings for SCI

Remember that SCI briefings don't transfer. The clearance holder must be debriefed from the organisation they're currently in before they are transferred. They must also be briefed into the organisation they're transferring to if they'll be accessing SCI.

Notifying the NZSIS when you transfer a security clearance

Your organisation must notify the NZSIS when the security clearance transfer has occurred.

When the transferred clearance expires

The transferred national security clearance will stop 5 years from the date of the original recommendation, or from when the original organisation granted the clearance.

Cancel their security clearance

When a clearance holder leaves your organisation, you should cancel their clearance and notify the NZSIS that you no longer employ the clearance holder.

Appendix 1: Security clearance levels

The four security clearance levels and their requirements are set out below.

CONFIDENTIAL Vetting (CV)

Assessment type	Candidate's suitability for ongoing access to New Zealand Government information or resources protectively marked at the CONFIDENTIAL level.
Nature of vetting	Vetting at the CONFIDENTIAL level is 'negative' in that inquiries are usually limited to checking records for adverse indicators. If nothing negative is found, the national security clearance will usually be recommended.
Checkable background requirement	Most recent 5 years of candidate's background, or to age 18 (unless requesting organisation provides compelling reasons otherwise)

SECRET Vetting (SV)

Assessment type	Candidate's suitability for ongoing access to New Zealand Government information or resources protectively marked at the CONFIDENTIAL level and SECRET level.
Nature of vetting	Vetting at the SECRET level is an 'intermediate' vetting involving more extensive enquiries than for a 'negative vetting'. The consideration not only assesses whether anything adverse is known about the candidate, but must also establish some positive assurance.
Checkable background requirement	Most recent 10 years of candidate's background, or to age 18 (unless requesting organisation provides compelling reasons otherwise)

TOP SECRET Vetting (TSV)

Assessment type	Candidate's suitability for ongoing access to New Zealand Government information or resources protectively marked at the CONFIDENTIAL, SECRET, and TOP SECRET level. This includes resources that carry compartmented markings.
Nature of vetting	For vetting at the TOP SECRET level, the security assessment must be 'positive'. Extensive inquiries are carried out to check suitability for access to the highest levels of national security information or resources that are protectively marked. Positive assessment is only given if inquiries provide sound reasons to consider the candidate trustworthy in the security context and suitable to have access to the highest levels of national security information.
Minimum age	18 years of age
Checkable background requirement	Most recent 10 years, or to age 18 (unless requesting organisation provides compelling reasons otherwise)

TOP SECRET SPECIAL Vetting (TSSV)

Assessment type	Suitability for ongoing access to all information and resources protectively marked under the security classification system, including resources that carry compartmented markings.

Nature of vetting	TOP SECRET SPECIAL clearance is limited to:
	• members of the New Zealand Intelligence Community (NZIC)
	• some groups and individuals within:
	  ○ the Department of the Prime Minister and Cabinet (DPMC)
	  ○ New Zealand Customs Service
	  ○ Ministry of Foreign Affairs and Trade (MFAT)
	  ○ New Zealand Defence Force (NZDF)
	• some agency heads who will have frequent access to the highest levels of national security information and a wide need-to-know requirement.
	
	More extensive inquiries are conducted in these instances.
	
	The final assessment must be compellingly positive, and have no residual security concerns.

Minimum age	18 years of age
Checkable background requirement	Most recent 15 years, or to age 18 (for initial clearance)