PSR | Protective Security Requirements

Guide to managing national security clearance holders

FEBRUARY 2018

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 (CSOs), security staff and 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, temporary 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 to access information, assets or premises classified CONFIDENTIAL, SECRET, or TOP SECRET must first be granted a national security clearance by your chief executive, or their delegate.

The requirement for a national security clearance relates to a role not an individual. The level of clearance is based on the security classification of information, assets or premises that a person needs to access to fulfil their duties — not on rank, seniority, or status. An organisation decides which duties and tasks require a person to have ongoing access to information, assets or premises classified CONFIDENTIAL or above and, therefore, to hold a national security clearance.

The government expects that the number of people who require national security clearances to perform their work will be kept to a minimum.

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

Roles in granting and managing clearances

Your organisation's chief executive is responsible for granting national security clearances and managing risk. This function may be delegated, for example to the Chief Security Officer.

The NZSIS is responsible for the security vetting process and for making recommendations on whether or not to grant a national security clearance.

The need-to-know-principle

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

Before granting access, an organisation must establish the existence of a legitimate need to access the protectively marked information, resources or classified premises to carry out official duties.

An organisation must only allow access to, and disseminate, protectively marked information or resources:

- to people who need to use or access the information or resources to do their work
- for ongoing access to people who hold the appropriate level of national security clearance.

Being in a position of authority or wishing to enter controlled areas because doing so is convenient are not sufficient justifications.

The organisation should 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.

More information

→ See ‘Appendix 1: Security clearance levels’ for more information.

The different levels of vetting needed for national security 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
- the breadth and depth of inquiries
- the time required to complete inquiries
- the time required to carry out assessments and make recommendations
- the degree of assurance of the candidate’s trustworthiness, honesty, and loyalty to New Zealand.

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 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 national security 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 national security clearance.

Your organisation must also notify the NZSIS of any:

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

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

Identify the need for a clearance

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

Grant a clearance

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

Set the right expectations

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

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 and assets.

Manage their departure

When a national security 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 outsourced service providers, require a national security clearance due to the information they have access to. In that case the national security clearance must be sponsored by a government organisation.

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

More information

→ Supply chain security

Identify the need for a clearance

People who are responsible for the creation, use, discussion, handling, storage, or disposal of material protectively marked CONFIDENTIAL or higher must hold a national security clearance at the appropriate level.

People do not require a clearance for access to material protectively marked IN CONFIDENCE, SENSITIVE or RESTRICTED, but the “need to know” principle still applies. Your organisation grants access to such material on the basis of its own personnel security checks.

To determine whether a person requires a national security clearance, and at what level, you should analyse the duties of the position and the highest level of classified information, resources or premises the person will access. If the classification is CONFIDENTIAL or above, the person must obtain a national security clearance. You should consult you organisation’s security staff throughout this process.

When someone needs to access classified information held on a network

All people who access protectively marked information communications technology (ICT) networks must have at least the highest level of clearance required to access information held on those networks.

If the networks are compartmentalised, then a person’s clearance level must match the highest-level compartment they can access. We recommend that your organisation seeks advice from the Government Communications Security Bureau (GCSB) before you determine the clearance levels required for compartmentalised systems.

Grant a clearance

Where a person will have regular and ongoing access to protectively marked information and resources at CONFIDENTIAL, SECRET or TOP SECRET level, your chief executive, or their delegate, must first grant a national security clearance at the appropriate level.

Your chief executive can only grant a national security clearance after receiving a security vetting recommendation from the NZSIS.

Security vetting is the process the NZSIS uses to assess a person's loyalty to New Zealand, integrity and trustworthiness, and suitability to access national security information. The process starts once your organisation raises a request for security vetting.

Your organisation must not use the security vetting process as a general trustworthiness check for current or potential employees or contractors.

Recruitment for positions that require national security clearances

When your organisation advertises a position, it is good practice to advise potential candidates that the position requires a national security clearance, and to include an outline of the eligibility criteria or a link to the eligibility criteria in the PSR.

This may deter candidates who are ineligible or unwilling to undergo the security vetting process from applying for the position.

National security clearance as a condition of employment

It is good practice to make the requirement to obtain and maintain a national security clearance a condition of employment.

Ideally, your organisation will have notified potential candidates of this requirement at the time of advertising. If your organisation has not done this, you should advise your chosen candidate before you offer them employment and include the requirement in their employment contract.

Eligibility for security vetting

Only New Zealand citizens or holders of a Residence Class visa should be put forward for security vetting. In exceptional circumstances other candidates may be considered for security vetting. You should discuss these cases with the NZSIS before submitting a vetting request.

Some organisations apply stricter criteria when deciding which people they will sponsor for a national security clearance based on their own specific assessment of risk.

Checkable background requirements

The backgrounds of vetting candidates must be checkable for the required period:

- 5 years for CONFIDENTIAL level clearances
- 10 years for SECRET and TOP SECRET level clearances

- 15 years for TOP SECRET SPECIAL level clearances.

Your Chief Security Officer (CSO), or their delegate, must ensure that each vetting candidate meets the minimum requirements for checkable history before submitting a vetting request.

If a candidate has spent a considerable period of their adult life outside New Zealand, your CSO, or their delegate, must discuss the candidate's background with the NZSIS before submitting a vetting request.

If the NZSIS is unable to make meaningful and reliable checks in the candidate's country or countries of residence, it will be difficult to make an accurate and reliable vetting assessment and the NZSIS may not accept the vetting request.

Foreign nationals

Foreign nationals are not permitted to access material that carries the endorsement marking NEW ZEALAND EYES ONLY (NZEO) and the security classification CONFIDENTIAL, SECRET or TOP SECRET, even if they have the appropriate New Zealand security clearance.

In limited circumstances, agencies may allow information marked NZEO to be viewed by appropriately cleared foreign nationals where there is an essential business need. In all such circumstances, the Director of Security, NZSIS must grant approval for this access.

Your organisation must not allow a foreign national granted a national security clearance to access protectively marked material originating from a third country unless that country has specifically approved the release.

If your organisation grants a national security clearance to a foreign national, it should place a condition on the candidate's employment that they gain New Zealand citizenship by a specific date.

More information

→ New Zealand Government Security Classification System

Request for the NZSIS to do a security vetting

Your organisation must have trust and confidence in the candidate and that candidate's ability to gain a favourable recommendation for a national security clearance before submitting a security vetting request to the NZSIS.

Your organisation's CSO, or their delegate, must review organisation holdings (such as performance or disciplinary records) before submitting a vetting request to ensure that nothing that your organisation already knows indicates that the candidate may be unsuitable for access to protectively marked information or resources.

Indications that the candidate may be unsuitable for a security clearance may be shown by a record of:

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

Also, if your organisation considers the candidate does not possess the strength of character and integrity needed to access protectively marked information or resources, your organisation should not submit the request for change in security clearance to the NZSIS. Your organisation must authorise all requests to the NZSIS for security vetting. Requests must be made using the Online Vetting Request (OVR) system.

More information

For more details on specific areas of concern and mitigating factors go to:

→ Security Assessment Criteria and the Adjudicative Guidelines

Urgent vetting requests

The NZSIS will give priority to urgent vetting requests. Your organisation should contact the NZSIS to discuss an urgent request before sending it.

When lodging requests for urgent vetting, your organisation must include:

- a brief description of the circumstances that make the vetting urgent
- the date by which a response from the NZSIS is required.

Your organisation 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.

Urgent vetting requests are processed on the basis of the age of the case, requirement of position, or other issues (not time-specific) that are only given urgent status in exceptional circumstances. Bear in mind that prioritising one vetting request is likely to delay other requests.

Your organisation must not grant a ‘waiver’, ‘interim’ or ‘temporary’ security clearance to the candidate before receiving the NZSIS’s recommendation.

New Zealand security vetting recommendations

The NZSIS will advise your organisation’s CSO when a security vetting is completed.

The clearance may be recommended:

- at the level requested
- at a lower level
- with specific security clearance management provisions (‘qualifications’).

Your organisation’s CSO must advise the NZSIS of their decision.

Action when clearance is granted at the requested level

Once clearance is granted, your organisation must provide the clearance holder with:

- a briefing on their responsibilities when handling information
- requirements for reporting any change in circumstances or suspicious contacts
- details of your organisation’s security awareness training programme.

Action when clearance is not recommended

Your organisation should not grant a security clearance when they receive an adverse recommendation from the NZSIS about the candidate.

Action when the clearance is not granted, or granted at a lower level

Your organisation must withdraw any access to protectively marked information or resources above the level of the clearance recommended, if any, until any reviews or appeals are finalised (see below).

If the NZSIS has concerns that may lead to a recommendation other than a security clearance at the requested level, they will give early advice to your organisation’s CSO to withdraw access.

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

Your organisation can then:

- confirm the employment condition is met
- take appropriate action to withdraw the offer of engagement, redeploy the person, or terminate the employment.

Action when candidate requests a review of recommendation

If the candidate requests that a recommendation is reviewed or appealed, your organisation should:

- withdraw any access to protectively marked information or resources above current clearance level until any reviews or appeals are finalised
- seek legal advice before deciding whether to continue with or withdraw an offer of employment, redeploy the person, or take other action.

Your organisation's CSO should notify the person's manager of the outcome, giving no more details about any qualifications to the clearance than those needed to manage the person effectively.

Specific recommendations for security risk management

Your organisation should observe any specific recommendations for security risk management ('qualifications') that the NZSIS makes.

Advice to the NZSIS

Your organisation must advise the NZSIS whenever it grants, declines, downgrades, suspends or cancels a security clearance.

Advice to candidates of their right to complain

A vetting candidate has a statutory right of complaint to the Inspector-General of Intelligence and Security if they consider any act, omission, practice, policy or procedure of the NZSIS has adversely affected them.

Your organisation's CSO must advise candidates of this right.

Complaints must be made 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

→ www.igis.govt.nz

Set the right expectations

A clearance holder's manager must communicate with them clearly to set the right expectations for their role.

The clearance holder must understand your organisation's security policies and practices, and be aware of them when they change.

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

A clearance holder needs to understand and acknowledge the specific responsibilities they have as a national security clearance holder. Their manager should clarify with them if their continued employment is conditional on them maintaining a clearance to the appropriate level.

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, clearance holders should 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 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.

→ Personnel security risk management plan template (under development - Contact Security Vetting for assistance)

Conduct security briefings as needed

Types of briefings that may be given 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 purposes
- briefings and debriefings for accessing TOP SECRET material
- briefings and debriefings to allow access to specific protectively marked information or resources that have an endorsement, are compartmented or have codeword protection (Note: some of these briefings need to be provided by NZSIS or GCSB)
- specific location briefings for high-risk destinations
- 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

Personnel security must be considered throughout the 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
- report any suspicious contacts.

The clearance holder's organisation must:

- provide annual security education
- conduct security briefings
- report and investigate security incidents
- manage emergency access to classified material
- report changes to the clearance holder's security clearance level
- review the clearance holder's security clearance.

Help them meet their responsibilities

You can help a clearance holder by providing them with security awareness and education, and handling any reports in 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 organisation's security requirements
- outline all legal, regulatory, and compliance requirements
- ensure they understand their security responsibilities.

Provide yearly security awareness and security briefings

Your organisation should provide security awareness training to clearance holders yearly.

Your organisation should conduct additional security briefings or debriefings (see 'Conduct security briefings') with clearance holders when appropriate.

Prepare for international travel

When your people 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. New Zealanders, especially Government officials, travelling overseas may be of interest for a number of reasons, including our:

- 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 subject to significant foreign investment interest
- defence and intelligence capabilities.

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

More information

→ Go to Maintaining your national security clearance to find Advice for New Zealand Government officials travelling overseas

Report changes in their personal circumstances

National security clearance holders must report any significant changes in personal circumstances to ensure that such changes do not affect their trustworthiness as a clearance holder.

What 'significant change' means

The following changes in a clearance holder's circumstances are significant and must be reported.

- Entering into, or ceasing, a close personal relationship
- Residence in, or visits to, foreign countries
- Relatives residing 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

→ Ensure their ongoing suitability

Advise the Chief Security Officer of any concerns

Clearance holders must report any significant change in their personal circumstances to your organisation's CSO and to their manager as soon as it happens. This reporting requirement helps to mitigate any possible conflicts of interest.

Managers should report any significant change in circumstances relating to a clearance holder to the CSO if they are unsure whether the clearance holder has notified the CSO of the change.

Your organisation's people should also report any significant changes in the circumstances of other people to their CSO if they believe a change may affect that person's suitability to retain a security clearance or uphold your organisation's security standards.

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

Recognise consequences of reporting a change in circumstance

Early recognition of a change in circumstance will usually allow the issue to be dealt with before it becomes a security concern, reducing the risk to the clearance holder and your organisation.

When a significant change in circumstance is identified or reported, your organisation must conduct a risk assessment based on whether the person can continue to hold a clearance. If this continuation is in doubt, your organisation should suspend or cancel the holder's national security clearance until the risk is mitigated or assessed as void.

Your organisation's CSO must assess the situation and, if necessary, escalate the matter to the NZSIS. Not all changes in personal circumstances will require this action. When the change is considered significant or is likely to present a risk to national security, your organisation must notify the NZSIS.

The NZSIS may consider it necessary for your organisation to submit a new vetting request. If the NZSIS is satisfied that the clearance holder remains suitable to retain a clearance at the particular level, 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 assets or protectively marked information, assets or work locations to their CSO.

Instances of suspicious contacts or requests include, but are not limited to, contact with foreign officials and foreign nationals, criminal groups or people, or other suspicious people.

Complete a contact report to report a suspicious contact

A clearance holder should complete a contact report when a contact has occurred that appears suspicious, persistent, or unusual in any respect, or becomes ongoing (whether in an official or social capacity) with:

- embassy or foreign government officials within New Zealand
- foreign officials or nationals outside New Zealand, including trade or business representatives.

Also, they should complete a contact report when any individual or group, regardless of nationality, seeks to obtain official information for which they do not have a valid 'need-to-know'.

More information

→ Go to Maintaining your national security clearance to find a Contact reporting form.

Assess the suspicious contact

Your organisation should assess the clearance holder's reported contacts to determine whether you need to:

- collect contact reports from other concerned people, and assess those reports
- advise the NZSIS of contacts the clearance holder has had that may have national security implications
- do an internal investigation (see Reporting Incidents and Conducting Security Investigations)
- forward any suspicious reports about national security to the NZSIS
- 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 (e.g. NZ Police, Serious Fraud Office) for further investigation.

More information

→ 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 access to emergency materials, and managing changes to their security clearance level.

Monitor concerning behaviour

A manager of a clearance holder must monitor the holder's 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 the manager must act within their normal 'duty of care' responsibilities.

If a clearance holder's manager finds a behavioural issue, they 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

The effective management of security incidents and investigations is a basic part of good security.

Your organisation has specific reporting requirements for breaches and violations. 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 protectively marked information
- security violations, including a deliberate action that leads, or could lead, to a compromise of protectively marked information or resources.

Provide details of security breaches to the NZSIS

If a clearance holder regularly infringes or breaches security, your organisation should provide the NZSIS with details of further infringements or breaches.

In the event of a security violation your organisation must inform the NZSIS.

In most instances, a security violation will result in your organisation initiating a review for cause (see below). You should also provide the NZSIS with all relevant details including details of any investigation under way (where privacy concerns allow).

Suspend access if necessary

Review for cause

A ‘Review for Cause’ is an early review of a security clearance holder, undertaken by the NZSIS, when security concerns have been identified 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 national security 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.

If the clearance holder is being investigated for a security violation, their manager should suspend their access to protectively marked information or resources 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 the national security clearance of a clearance holder if they consider the security concerns, breaches or violations are too frequent or of a sufficiently serious nature.

More information

→ Reporting Incidents and Conducting Security Investigations

Manage their emergency access to classified material

Sometimes an emergency may give rise to an urgent operational need for a clearance holder to access protectively marked information or resources above their clearance level.

'Emergency access' means:

- access where an urgent and critical operational need for access to particular material is established and there is insufficient time to complete vetting inquiries and grant a higher level clearance
- access only to specified material required for the particular emergency
- access for no longer than the duration of the emergency
- access governed by a very strict application of the need-to-know principle.

Grant temporary supervised access

During an emergency, a clearance holder's chief executive, or their delegate, has the authority to grant a clearance holder temporary supervised access to protectively marked information or resources one level above their current national security clearance level. For example, if their current clearance is CONFIDENTIAL, their manager may supervise them to view SECRET material while the emergency lasts.

The manager must confirm this access in writing, and brief the clearance holder appropriately. The clearance holder must acknowledge that their manager has briefed them before being granted access. Your organisation must also debrief the clearance holder when the emergency ends.

A clearance holder's manager 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 protectively marked information or resources that carries an endorsement or compartmented marking.
- A clearance holder's manager must not grant a non-clearance holder emergency access to material protectively marked CONFIDENTIAL or higher.

Manage changes to their security clearance level

Sometimes the clearance holder's national security clearance level or status will change. The holder's manager must advise the NZSIS when your organisation grants, upgrades, downgrades, renews, suspends, cancels, or transfers a national security clearance.

Review after five years

A clearance holder's national security clearances will expire after five years (or sooner if the NZSIS has recommended an early review) or when the holder leaves their employment.

The clearance holder's manager is responsible for managing the process to ensure the holder's ongoing security clearance, even if the clearance level changes.

When reviewing a clearance holder's suitability to hold a clearance, the reviewer must have trust and confidence in the holder's ability to gain a favourable recommendation before submitting a security vetting request to the NZSIS. To make such an assessment, the reviewer must exercise their own judgement, and view all information available to them objectively.

Your organisation should initiate a review of a national security clearance by the NZSIS early enough to maintain continuity of the security clearance unless:

- the person is no longer in a position requiring a security clearance, or
- the person has left New Zealand government employment.

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 resources protectively marked at a higher level than their current clearance, they must undergo security vetting at that higher level.

The holder's manager 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 level clearance granted by your chief executive, or their delegate, 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.

Alternatively, concerns may emerge that mean a clearance needs downgrading. Also see 'Review for cause' earlier in this guide.

Depending on the outcome of the downgrade process, a manager must:

- confirm that the downgraded security status meets the clearance holder's employment condition
- take appropriate action to redeploy the clearance holder or end their employment.

Note: Your organisation must seek legal advice in cases of redeployment or termination.

The clearance holder is entitled to request a review to discuss, or lodge an appeal against, the proposed downgrade. They can only do so at the end of the appeal or review process.

Also see 'Action when candidate requests a review of recommendation' under earlier section about 'New Zealand security vetting recommendations'.

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

See these sections in the earlier section on 'New Zealand security vetting recommendations':

- Action when the clearance is not granted, or granted at a lower level
- Action when candidate requests a review of recommendation.

Manage the clearance holder's 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 a clearance holder leaving an organisation, their manager must:

- remind them of their ongoing obligations
- debrief them from for any access to compartmented information
- transfer or cancel their security clearance
- notify the NZSIS.

Depending on their clearance level and briefings they hold, an appropriately cleared and briefed person may have to:

- debrief the holder for any access to compartmented information
- 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, and
- their lifelong obligation to protect protectively marked information or resources.

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, when the clearance transfer process has been followed.

The chief executive of the new organisation may grant the clearance holder a new clearance. This action will happen immediately, provided the following conditions are met:

- the original clearance is less than five years old
- However, if the original clearance is more that four years old at the time of transfer the new organisation should immediately begin the process to renew the clearance
- there is a requirement to access protectively marked information or resources or locations in the new role
- the transferred national security clearance is at the same level or at a lower level than the clearance originally granted

- 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, or their delegate, obtains from the clearance holder's old organisation:
- a copy of the NZSIS's vetting recommendation (this may have important security risk management advice)
- written assurance of the clearance holder's continuing suitability to hold a national security clearance
- notification of any relevant changes in the clearance holder's personal circumstance since being initially assessed, and confirmation that the NZSIS has been notified of these changes.

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

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

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

Cancel their security clearance

A national security clearance will normally be cancelled when the holder leaves their employing organisation.

Your organisation must notify the NZSIS that the organisation no longer employs 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	20 years of age
Checkable background requirement	Most recent 10 years, or to age 18 (unless originating organisation provides compelling reasons otherwise)

TOP SECRET SPECIAL Vetting

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