PSR | Protective Security Requirements

Version: 1.0 ***Last Review Date: Oct 2025***

Protective Security Requirements (PSR) Policy Framework:

PERSONNEL SECURITY (PERSEC)

MANDATORY REQUIREMENTS 1-4

Introduction for document reviewers

What is this document?

This document is the final V1.0 consolidated PSR policy framework on personnel security (PERSEC) implemented on 01 October 2025. It replaces all previous PSR policy requirements published on the PSR website.

Why has this document been developed?

In the past, PSR policy requirements were expressed on the PSR website and in publications, rather than in authoritative policy framework documents. Similar and overlapping content was spread across multiple webpages and at times expressed unclearly. This made PSR policy requirements difficult for stakeholders to find, understand, and apply.

This document aims to resolve these issues by establishing a clear and appropriate policy framework for personnel security. Separate policy frameworks have been developed for other PSR domains.

What is this document based on?

This consolidated policy framework compiles the personnel security policy requirements previously set out on the PSR website, Capability Maturity Model, and relevant PSR guidance publications.

The content is structured according to the mandatory requirements, with consistent use of sub-headings within each mandatory requirement and numbered paragraphs.

The security measures required to comply with the PSR are expressed clearly, using MUST, SHOULD, and COULD statements.

The intent of this consolidated PSR policy framework is to clarify existing requirements, and to better support agencies to check that they are meeting these requirements. The intent is not to introduce significant or substantive change to these requirements.

Some policy requirement changes have been made, including those required to:

- resolve inconsistencies resulting from repetition and duplication of content
- incorporate essential elements (including from personnel security printed materials)
- align with broader expectations or existing practice.

Has the minimum baseline for PSR changed?

The policy framework has been reviewed and clarified to ensure that it remains a robust protective security policy framework aligned with security best practice. The policy framework now articulates the minimum set of security capability and measures required for all organisations no matter their level of risk.

The minimum requirements are expressed as MUST statements and has been aligned to the PSR Capability Maturity (PS-CMM) level of 2 “Planned and Tracked” (formerly called ‘Basic’).

Table of Contents

Purpose

1. The purpose of this policy framework is to support organisations to set up effective personnel security measures to protect its people, information, and assets. The framework covers personnel working within an organisation (including employees, contractors, temporary staff, and secondees.)

Who should read this document

2. This policy framework is primarily intended for use by organisations that implement the Protective Security Requirements (PSR). This includes:
    a. government organisations that are mandated to implement the PSR, and
    b. organisations that implement the PSR on a voluntary basis.
3. As good security practice, non-mandated organisations in the public and private sectors are encouraged to adopt the PSR as appropriate to their context.
4. This policy framework should be read along with the PERSEC Appendices, PSR Information Security (INFOSEC), PSR Physical Security (PHYSEC), and PSR Security Governance (GOV) policy frameworks.
5. This information should be used by leaders and those with functional responsibility for protective security to establish their own security policies and measures to address their risks.

Introduction to the PSR

6. The PSR is New Zealand's best practice policy framework. It sets out what an organisation must do to manage security effectively. It also contains best practice guidance. See PSR Policy Framework Overview for a summary of the PSR policy requirements.

7. Protective security is a business enabler. It allows organisations to work together securely in an environment of trust and confidence, to maintain public trust and confidence, and to support strategic and operational objectives.

Required and recommended measures

8. The PSR describes when an organisation needs to consider specific security measures – also called "controls" – to comply with mandatory requirements.

9. The measures required depend on the level of risk to be managed.

Required measures

10. A measure expressed with 'MUST' (or 'MUST NOT') is mandatory for all levels of risk. An organisation MUST implement all mandatory measures unless it can demonstrate that a given measure is not relevant in its context.

11. A measure expressed with 'MUST consider' requires that in developing the organisation's policies, an organisation has considered if and when the measure applies. Considerations must be documented.

12. If a mandatory measure cannot be directly implemented unless expressly stated otherwise, suitable compensating measures MUST be selected to manage identified risks.

Recommended measures

13. A measure expressed using 'SHOULD' (or 'SHOULD NOT') is recommended for organisations with moderate and above risks.

14. A measure expressed using 'COULD' is recommended for organisations with high and above risks.

15. Valid reasons for an organisation not implementing recommended measures could include:

    a. a measure is not relevant because there is no apparent risk, or

    b. the residual risk is acceptable, or

    c. an alternative measure of equal strength is in place.

16. Not using recommended measures without due consideration may increase residual risk for an organisation. This residual risk needs to be agreed and acknowledged by an organisation head. Pose the following questions before choosing not to implement a recommended measure.

a. Is the organisation willing to accept additional risk? If so, what is the justification for this choice?

b. Has the organisation considered the implications for all-of-government security? If so, what is the justification for this choice?

17. A formal auditable record of how an organisation considers and decides which measures to adopt is required as part of an organisation's governance and assurance processes.

Compliance with legislation

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

Why personnel security matters

19. Although people can be an organisation's greatest asset, they can also be a weakness.

20. Personnel security protects people, information, and assets by enabling an organisation to:

a. reduce the risk of harm to its people, customers, and partners

b. reduce the risk of your information or assets being lost, damaged, or compromised

c. have greater trust in people who access official or important information and assets

d. deliver services and operate more effectively.

21. Personnel security focusses on reducing the risks associated with insider threat. Insider threats come from past or present employees, contractors, or business partners. Insiders can misuse their inside knowledge or access to harm an organisation's people, customers, assets, or reputation.

22. Insider acts do happen here in New Zealand and the consequences are severe. The threat is real and we're all responsible for helping to reduce the risks. The PSR Unit developed a security campaign It happens here: Managing the insider threat to your organisation. This campaign is designed to help raise awareness of insider threat in the workplace. Where appropriate, an insider threat program may be necessary to address insider risks.

Personnel Security Policy Framework

23. Robust security practices are required to protect an organisation's people, information, and assets. When an organisation's personnel security measures are well designed and implemented, it reduces the risk of insider threat.

24. An organisation needs to understand and effectively manage personnel security risks across the personnel security risk management cycle (PDF) to reduce the risk of insider threat. The ongoing cycle consists of three key activities:

    a. assess personnel security risks

    b. manage personnel security risks, and

    c. evaluate how effectively personnel security risks are managed.

Assess personnel security risks

25. As part of GOV2 (Take a risk-based approach), an organisation MUST identify potential sources of personnel security risk, including the way these risks may present and the types of threat they pose.

26. The risk assessment SHOULD identify roles, or groups of personnel (including contractors), who have greater potential to cause harm due to their access to sensitive, valuable or classified information or assets. Examples of insider threat risk include;

    a. unintentional or deliberate disclosure of information

    b. loss of intellectual property

    c. privacy breaches

    d. theft/dishonesty, and

    e. personal gain from official actions (conflict of interest).

Manage personnel security risks

27. Each stage of the personnel lifecycle presents distinct challenges. An organisation needs to consider personnel security from the time recruitment/procurement has begun, when a person is hired or engaged, and through to the moment they leave an organisation – possibly even after they leave.

28. To manage personnel security risks, an organisation MUST continually and consistently apply security measures to all people working for the organisation.

Evaluate how effectively risks are being managed

29. As part of GOV8 (Assess your capability), an organisation MUST evaluate if security arrangements and practices are still effective. What works well and what does not should be identified and arrangements adjusted accordingly.

30. Threats faced by an organisation change over time. As part of GOV2 (Take a risk-based approach), an organisation SHOULD consider whether its understanding of the sources of personnel security risk is accurate and up to date.

PERSEC Mandatory Requirements Overview

31. Building on the personnel security risk management cycle above, the four PERSEC mandatory requirements help to ensure that access to information and assets is only given to suitable people. These are:

    a. PERSEC 1 – Recruit the right person

    b. PERSEC 2 – Ensure their ongoing suitability

    c. PERSEC 3 – Manage their departure, and

    d. PERSEC 4 – Manage National Security Clearances.

32. Public service agencies and statutory Crown entities mandated to follow the PSR MUST adopt all PERSEC mandatory requirements.

33. Additionally, *all* public sector agencies and statutory Crown entities are required to follow PERSEC 1 under the Public Service Commission's Workforce Assurance Model Standard. This standard outlines additional expectations on organisations when recruiting staff, investigating serious misconduct, and use of settlement agreements (including confidentiality and non-disclosure statements).

34. As good practice, private sector organisations may adopt the PERSEC mandatory requirements.

PERSEC 1: Recruit the right person

Ensure that all people working for your organisation (employees, contractors, and temporary staff) who access New Zealand Government information and assets:

- have had their identity established
- have the right to work in New Zealand
- are suitable for having access
- agree to comply with government policies, standards, protocols, and requirements that safeguard people, information, and assets from harm.

35. Pre-employment checks are the foundation of good personnel security. They reduce the risk of a trusted person harming an organisation. Pre-employment checks allow an organisation to:

    a. confirm the identity, eligibility, suitability, and capability of a person being recruited, and
    b. find out if an applicant has concealed important information or misrepresented themselves.

36. Privacy and employment laws apply to an organisation or a third-party gathering information from referees or other sources, and consent is required from the applicant.

37. An organisation needs to ensure that pre-employment checks are carried out on personnel it is considering directly employing or otherwise engaging, including contractors, temporary staff, secondees, and existing employees moving between roles (herein referred to as 'personnel'.)

38. An organisation may get a third party, such as a recruitment agency, to do all or some of the checks for them. When using a third party, consider obtaining:

    a. confirmation that the third party has completed the requested checks
    b. copies of reference checks or other evaluative material, and
    c. any other assurance deemed necessary.

39. An organisation needs to undertake the mandatory pre-employment checks required for all applicants for national security clearance applicants (see PERSEC 4).

PERSEC 1.1: Carry out baseline checks for all roles

PERSEC 1.1.a Confirm identity and nationality

40. An organisation MUST confirm the identity and nationality of personnel they are considering employing (or otherwise engaging).

41. Confirmation of a candidate's identity and nationality MUST be undertaken by sighting an original document where practicable, such as a passport or birth certificate. When confirming a person's identity, consider:

    a. some people may have an alias, such as previous family name
    b. some people may be known by other first names, and
    c. naming conventions differ between cultures.

42. If an organisation finds unexplained discrepancies in someone's identity documentation, it SHOULD seek further advice.

43. Refer to the Identification Standards set by the Department of Internal Affairs (DIA) for more information.

PERSEC 1.1.b Confirm the right to work in New Zealand

44. If recruiting someone in New Zealand, an organisation MUST ensure that the candidate is either a New Zealand citizen or has a visa that allows them to work in New Zealand.

45. For candidates who aren't New Zealand citizens, the organisation MUST check which visa they hold and whether visa conditions prevent them to do the job they're applying for. See Immigration NZ's VisaView system for assistance.

46. If an organisation is recruiting someone to work in an overseas location, it MUST check the applicant has the right to work in that country. For example, if an organisation is recruiting for its Australian-based office, it MUST confirm the applicant is eligible to work in Australia.

PERSEC 1.1.c Check references with former employers

47. How a person has performed and behaved in the past is a good indicator of their future performance and behaviour. Checking references thoroughly gives an organisation an opportunity to:

    a. check the person can do what they say they can, and
    b. gain insight into the person's character.

48. An organisation MUST verify that a prospective employee worked for their previous employer as evidenced in their CV, and MUST obtain references from referees that are:

    a. recent, including from the most recent employer
    b. appropriate for the role
    c. from a legitimate source, and
    d. free from any conflicts of interest (such as being in a close personal relationship with the applicant).

49. To help with checking suitability of current employees, an organisation MUST review its records (such as performance or disciplinary records). Any records that show dishonesty, misconduct, or breaches of the Code of Conduct may reveal the person to be potentially unsuitable.

50. If an organisation has concerns after checking references or other records, but wishes to progress the person's candidacy nevertheless, it MUST consider conducting additional optional pre-employment checks (see PERSEC 1.2 for additional optional checks).

PERSEC 1.1.d Conduct a criminal record check

51. A criminal record check (Ministry of Justice check) helps an organisation to identify any:

a. criminal convictions not subject to the Criminal Records (Clean Slate) Act 2004 that may make a person unsuitable for the role, and
b. measures that may need to be put in place to manage risk if recruitment of the person proceeds.

52. An organisation MUST conduct a Ministry of Justice criminal record check on all prospective employees.

53. An organisation MUST have the person's consent in writing before progressing a criminal record check. An organisation MUST also understand its obligations as a potential employer.

54. If an organisation is concerned about the results of a criminal record check but wishes to progress a person's candidacy, it MUST consider conducting additional pre-employment checks to get a clearer picture of the person's trustworthiness and suitability.

55. When doing pre-employment checks for people who are overseas residents or recent migrants, the organisation MUST consider whether an overseas criminal record check is needed. The UK Home Office provides useful guidance on processes for obtaining criminality information from other international countries.

56. In some countries, only the person the criminal record belongs to can apply for their record. In this situation, an organisation may need to ask the person to apply for their record and to give the organisation an original or authenticated copy.

PERSEC 1.2: Conduct additional checks where an increased security risk is identified

57. Additional checks may be required to manage the additional risks individuals in specific roles may present. The additional pre-employment checks conducted will depend on various factors such as the organisation's security context and culture, legislated requirements, and operating environment.

58. Additional pre-employment checks may include:

a. psychometric testing
b. checks of qualifications and/or occupational registrations
c. credit checks
d. NZ Police check, and
e. drug and alcohol checks.

59. An organisation MUST have identified the roles requiring additional pre-employment checks based on legislated requirements and/or increased risk. For example, an organisation may decide to conduct additional pre-employment checks for an IT administrator who will have broad access to an organisation's information.

60. An organisation SHOULD have policies and procedures defined detailing when and how additional checks are undertaken to manage identified risks.

PERSEC 1.2.a Psychometric testing

61. An organisation COULD conduct psychometric testing if:

a. there is concern about the results from baseline pre-employment checks, or
b. it is difficult to assess whether the person has the abilities and traits required for the role.

62. Refer to Public Service Commission's advice on the use of psychometric testing in their guidance on eliminating bias and discrimination in recruitment (see section: Additional things to consider).

PERSEC 1.2.b Checks of qualifications and/or occupational registrations

63. If required for specific roles, an organisation MUST have policies and procedures for checking a person's qualifications (or occupational registrations) where they are critical to the role to be undertaken. Immigration NZ's website lists occupations that require registration in New Zealand and the contact details for authorities that can verify whether a person is registered.

64. An organisation COULD conduct a qualification check and/or a check of occupational registration to confirm that the educational qualifications, professional body memberships, or practising certificates claimed by the applicant are legitimate.

65. An organisation may want to confirm with the New Zealand Qualifications Authority (NZQA) on whether a qualification from overseas is recognised in New Zealand or comparable to a New Zealand qualification.

PERSEC 1.2.c Credit checks

66. A credit check is a commercial check of public records associated with the applicant's financial history and any associations with businesses. Bankruptcies are listed in the public Insolvency Register until four years after discharge.

67. An organisation COULD consider conducting a credit check if the role carries a significant financial risk. When conducting a credit check, an organisation should:

a. get the person's consent to undertake a credit check first
b. get an appropriately experienced person to review the results, and
c. have policies and processes to address any questions that a check brings up.

PERSEC 1.2.d New Zealand Police check

68. The New Zealand Police Vetting Service covers more than convictions. The New Zealand Police may release any information they hold if relevant to the purpose of the vetting request. This may include:

a. conviction history reports
b. infringement/demerit reports
c. active charges and warrants to arrest
d. charges that did not result in a conviction including those that were acquitted, discharged without conviction, diverted, or withdrawn
e. any interaction had with New Zealand Police considered relevant to the role being vetted, including investigations that did not result in prosecution
f. information regarding family harm where the applicant was the victim, offender or witness to an incident or offence, primarily in cases where the role being vetted

for takes place in the applicant's home environment where exposure to physical or verbal violence could place vulnerable persons at emotional or physical risk, and

g. information subject to name suppression where that information is necessary to the purpose of the vet.

69. An organisation SHOULD consider conducting New Zealand Police Vetting when doing so is consistent with the purpose of Police vetting. This may be a legislated requirement for specific roles. Refer to New Zealand Police for more information on the organisation's eligibility for Police Vetting.

PERSEC 1.2.e Drug and alcohol checks

70. An organisation may need legal advice before deciding to undertake drug and alcohol testing as privacy and employment laws apply.

71. An organisation COULD conduct drug and alcohol testing for roles which:

a. involve working in safety-sensitive areas, or
b. directly affect the safety of other people.

72. An organisation COULD decide these checks are appropriate when baseline checks suggest the applicant may have problems with drug or alcohol use.

PERSEC 1.3: Address any concerns from pre-employment checks

73. An organisation needs to be alert to warning signs from pre-employment checks. Factors that on their own, or together, may raise concerns about a person's integrity and suitability to work in an organisation, include:

a. any current involvement with criminal activity
b. withholding information about criminal convictions other than in accordance with the Criminal Records (Clean Slate) Act 2004
c. false statements in a CV or job application form
d. false claims about qualifications or achievements
e. unexplained gaps in the applicant's employment or residential history
f. adverse character references
g. conflicts of interest
h. evasive behaviour when asked to verify information they have provided
i. evasive behaviour of a refusal when asked to supply references or give consent for criminal record checks or credit checks.

74. If an organisation has any concerns arising from pre-employment checks, it SHOULD:

a. assess how the risks are likely to affect the role the person may be employed for, and
b. work out whether the risks can be reduced to an acceptable and manageable level.

PERSEC 1.3.a Create a risk management plan if necessary

75. If an organisation employs a person with identified personnel security risks, it SHOULD work with the person to create an individual risk management plan.

76. An organisation SHOULD use the individual risk management plan to support the person in their work, treat risks, and maintain organisational security.

PERSEC 1.3.b Record what is discovered

77. An organisation MUST record:

    a. checks completed
    b. concerns that come up during pre-employment checks
    c. risk assessments it carries out, and
    d. decisions it makes to reduce or manage risks.

PERSEC 1.4: Set the right expectations

78. An organisation MUST set clear expectations about security. The organisation must ensure new employees, employees changing roles, and contractors are informed of security policies and practices as soon as possible when joining the organisation.

79. To make sure everyone is aware of their responsibilities for security, an organisation MUST conduct an induction, including on organisational values, codes of conduct, health, safety and security procedures, and workplace expectations.

PERSEC 2: Ensure their ongoing suitability

Ensure the ongoing suitability of all people working for your organisation. This responsibility includes addressing any concerns that may affect the person's suitability for continued access to government information and assets.

80. People and their circumstances can change over time or suddenly as a reaction to an event. It is important to monitor your personnel's ongoing suitability. Managers and co-workers are in the best position to notice changes in a person's behaviour or attitude.

PERSEC 2.1: Minimum requirements to ensure ongoing suitability

81. To ensure ongoing suitability, at minimum, an organisation MUST have policies and procedures in place to:

    a. enable its personnel to report personnel security concerns and incidents
    b. assess and respond to relevant personnel security concerns and security incidents to ensure contain events and manage consequences
    c. provide ongoing security awareness updates and training.

82. An organisation SHOULD have clear guidelines and procedures for assessing and managing personnel suitability and integrity concerns, both at initial hiring and ongoing through their tenure.

83. Refer to GOV 4 (Build security awareness) and GOV 6 (Manage security incidents) for specific requirements to meet the minimum requirements.

84. An organisation SHOULD provide its personnel with access to support, such as a confidential employee assistance programme. An organisation SHOULD encourage its personnel to report and deal with personal issues before they become a serious problem.

85. An organisation SHOULD create policies and tools for managers to identify, support, and manage people who display concerning behaviour relating to security, poor performance, or unacceptable conduct.

86. An organisation COULD set up a dedicated internal wellbeing support service as part of a holistic programme to minimise insider risk.

87. An organisation COULD establish an insider threat programme aimed at effectively addressing insider risks.

PERSEC 2.2: Carry out ongoing suitability checks for higher risk roles

88. When an organisation identifies an increased security risk related to a role or the nature of its work, it may be necessary for an organisation to carry out additional ongoing checks. The checks applied will depend on a range of factors, including organisational security context and culture, and operating environment.

89. An organisation SHOULD consider the use of some the following ongoing suitability checks for higher-risk roles (including contractors):

a. requiring people to report any significant change in personal circumstances (for example, a divorce, new partner, bankruptcy, foreign citizenship, or new and significant debt)
b. requiring people to report any suspicious contacts (such as any social or official contact that appears suspicious, ongoing, unusual, or persistent in any respect)
c. encouraging people to report any suspicion of insider threat
d. carrying out an engagement survey to understand how satisfied and engaged the organisation's people are
e. briefing people on the risks related to international travel
f. requiring regular criminal record checks or NZ Police vetting as appropriate
g. carrying out periodic financial or credit checks
h. requiring drug and alcohol testing
i. checking regularly for conflicts of interest
j. obtaining copies of annual practising certificates.

90. An organisation SHOULD identify and manage insider risks associated with high-risk roles, or groups of people, who have greater potential to cause harm due to their access to sensitive, valuable, or highly classified information and assets.

91. An organisation COULD review role specific risk assessments regularly to confirm they are accurate and up to date (e.g. when role, personnel, process, information and/or system changes).

Higher-risk roles requiring a National Security Clearance have a different set of personnel security requirements as set out at PERSEC 4.

PERSEC 2.2.a Ensure significant changes in personal circumstances are reported

92. Significant changes in personal circumstances can arise from many different areas: relationships, finances, health, work issues, substance abuse, or new interests and contacts. These changes can put people under pressure and increase the risk of irrational or inappropriate behaviour or vulnerability to exploitation by others.

93. Having its personnel report significant changes in circumstances helps an organisation to manage the risk of someone (see also example Change in circumstance form):

a. having increased vulnerability due to changes in personal circumstances (e.g., relationships, finances, health, etc.)

b. breaching the organisation's security wittingly or unwittingly, or

c. being coerced into breaching an organisation's security by an external party.

94. An organisation SHOULD have policies and procedures for reporting changes in personal circumstances to ensure its personnel know which changes of circumstances they need to report and who they should report them to.

PERSEC 2.2.b Ensure suspicious contacts are reported

95. Foreign officials, foreign intelligence services, and commercial, political, or issue-motivated groups can devote considerable energy to accessing information (for

example, political, economic, scientific, technological, financial, and military information). Small pieces of information can all contribute to a valuable picture.

96. As part of GOV 4 (Build security awareness), an organisation needs to ensure its personnel understand that a seemingly innocent conversation or contact, such as an email, may be part of a wider intelligence gathering exercise. Contacts can be official (as part of a person's role) social, or incidental and can take place in a wide variety of contexts.

97. An organisation SHOULD ensure its personnel complete a contact report when an official or social contact appears suspicious, ongoing, unusual, or persistent (SOUP) in any respect. This contact could be with:

    a. embassy or foreign government officials within New Zealand

    b. foreign officials or nationals outside New Zealand, including trade or business representatives, or

    c. any individual or group, regardless of nationality, that seeks to obtain official or commercially sensitive information that are not authorised to access the information.

PERSEC 2.2.c Brief people on the risks related to international travel

98. When people travel overseas, they could be targeted by foreign intelligence services aiming to get access to New Zealand Government information.

99. As part of GOV 2, the organisation needs to identify roles, or personnel who have greater potential to cause harm due to their access to sensitive, valuable, or classified information or assets which could make them a target by foreign intelligence services.

100. To protect its own interests and those of New Zealand, an organisation SHOULD provide advice or brief its personnel in high-risk roles on the risks related to international travel and the security measures they need to take. Any measures taken to mitigate identified risks should be proportionate to the risk associated with the travel.

101. According to the organisation's policies for international travel, an organisation's relevant personnel SHOULD:

    a. consult the organisation's responsible person/team before travelling to check if a security briefing is necessary

    b. know what methods foreign agents may use to gather information

    c. understand how to protect the organisation's information and assets

    d. know what information they must protect

    e. know what information they can share and trade, and

    f. be aware of how to manage the organisation's electronic devices.

102. When returning from high-risk travel, an organisation SHOULD consider debriefing its personnel to check for any contact they had that appeared suspicious, ongoing, unusual, or persistent (SOUP).

103. For more advice refer: Security advice for New Zealand Government officials travelling overseas on business.

PERSEC 2.3: Manage role changes

PERSEC 2.3.a Undertake appropriate checks on personnel changing roles

104. It is common for people to enter an organisation in one role then move to another role with different responsibilities and/or a higher risk profile.

105. Before confirming an existing person into a different role, the organisation MUST make sure that all required pre-employment checks and/or on-going suitability checks have been completed to the level required for that role.

PERSEC 2.4: Manage contractors

106. Contractor access to information and assets comes with the same security risks as for permanent employees, as well as additional risks associated with their temporary appointment, potential conflicts of interest, and primary relationship to a third party.

107. To protect information and assets, an organisation MUST use the same personnel security measures with contractors as are applied to employees.

108. Consider extra measures to counter the security challenges that contractors can present. Refer to PSR Guide to hiring and managing contractors (PDF) for guidance on the additional risks and possible treatments for contractors across the personnel security lifecycle.

PERSEC 3: Manage their departure

Manage people's departure to limit any risk to people, information and assets arising from people leaving your organisation. This responsibility includes ensuring that any access rights, security passes, and assets are returned, and that people understand their ongoing obligations.

109. Managing departures well protects an organisation's security and reputation.

110. Whether a person is leaving by choice or not, a positive exit experience reduces the risk they will misuse their knowledge of business operations, intellectual property, official information, or any security vulnerabilities.

PERSEC 3.1: Remove access and collect assets

111. To manage departures, an organisation MUST:

    a. remove the person's permissions and ability to access electronic resources, documents, and physical sites

    b. ensure all identification cards and access passes are returned (including any tools that allow remote access to information systems), and

    c. ensure that all property belonging to the organisation is returned.

PERSEC 3.2: Conduct debriefs and confidentiality agreements

112. Where there is higher risk associated with a particular role or a person's circumstances, an organisation SHOULD conduct an exit debrief to:

    a. remind the person of any ongoing obligations relating to the organisation's people, information and assets, in particular intellectual property or official information, and

    b. invite them to discuss their reasons for leaving, and their perception of the organisation and its people.

113. An organisation COULD use a confidentiality agreement to protect the organisation's proprietary information or intellectual property.

PERSEC 4: Manage national security clearances

Ensure people have the appropriate level of national security clearance before they are granted access to CONFIDENTIAL, SECRET and TOP SECRET information, assets or work locations. Manage the ongoing suitability of all national security clearance holders to hold a clearance and notify NZSIS of any changes regarding their clearance.

114. Government organisations can sponsor personnel to hold a national security clearance to enable the granting of access to CONFIDENTIAL, SECRET, and TOP SECRET information, assets or work locations. Once granted, the government organisation becomes the sponsor of the clearance and is responsible for managing the clearance holder in accordance with PERSEC 4.

115. To manage national security clearances, an organisation needs to:

    a. identify, record, and review positions that require access to CONFIDENTIAL, SECRET, and TOP SECRET information, assets or work locations

    b. obtain a recommendation from the New Zealand Security and Intelligence Service Vetting Service (NZSIS Vetting Service) before granting a person a national security clearance

    c. check that the person has the right level of clearance prior to giving access to classified information, assets, or work locations

    d. ensure the ongoing suitability of all clearance holders to continue to hold a national security clearance, and

    e. manage all clearance holders' departure.

116. An organisation needs to notify the NZSIS Vetting Service of any:

    a. decision to grant or decline a national security clearance via the Vetting Security Clearance Lifecycle Management System (Tiaki)

    b. decision resulting in a change to a national security clearance via Tiaki (e.g., suspension, renewal, extension, transfer, sharing, downgrading, or cancellation)

    c. concerns that may affect the suitability of a person to obtain or maintain the appropriate level of clearance, or

    d. clearance holder who leaves the organisation or ends a contract with the organisation.

117. For an overview of the vetting process for applicants for a national security clearance, see Getting and maintaining a national security clearance.

PERSEC 4.1: Determine the clearance level needed

PERSEC 4.1.a Considerations for determining the required clearance level

118. If a person needs access to government information, assets, or work location classified as CONFIDENTIAL, SECRET, or TOP SECRET for their role, the organisation MUST ensure that that person holds a national security clearance at the appropriate level.

119. The level of clearance MUST be based on the security classification of information, assets or work locations that a person needs to access to fulfil their duties. It MUST NOT be based on rank, seniority, or status.

120. To determine whether a person requires a clearance and at what level, an organisation MUST:

    a. analyse the duties of the position

    b. identify the highest level of classified information, assets, or work locations the person will need access to

    c. identify whether the person will have access to any collections of classified information or assets (physical collections and collections of information in ICT systems), and

    d. decide how long the person will need the clearance for (i.e., a short-term or permanent role)

    e. consult its security staff throughout the process.

PERSEC 4.1.b Considerations for access to highly classified and sensitive compartmented information

121. As required by INFOSEC, anyone who needs access to an ICT system that holds classified information or assets marked CONFIDENTIAL or above MUST have a clearance that matches the highest protective marking of information held in the system.

122. If a system holds sensitive compartmented information (SCI), an organisation MUST ensure that everyone who accesses the system has the required security clearances and briefings for the compartments. Refer to the NZISM for more information on limits associated with access to SCI.

PERSEC 4.1.c Considerations for short term or temporary access

123. If a new clearance is needed for a short-term role, the organisation needs to contact the NZSIS Vetting Service about whether the person could be cleared in time to fulfil the position.

PERSEC 4.2: Determine eligibility and suitability for a national security clearance

124. The NZSIS Vetting Service helps to mitigate threats to national security by assessing if an applicant is trustworthy, and responsible to be granted a national security clearance.

125. Before an organisation can grant a national security clearance, it MUST receive a security vetting recommendation from the NZSIS Vetting Service.

126. Before an organisation submits a vetting request to the NZSIS Vetting Service for a national security clearance vetting assessment, it MUST check the applicant's eligibility and suitability.

127. An organisation's CSO (or delegate) is responsible for:

    a. making sure eligibility and suitability checks are done, and

    b. submitting vetting requests to the NZSIS Vetting Service.

128. See PERSEC Appendix A Security Clearance Levels for the four security clearance levels and their requirements. See PERSEC Appendix B Security Assessment Criteria and the Adjudicative Guidelines for the NZSIS' vetting process and Security Assessment Criteria and Adjudicative Guidelines.

PERSEC 4.2.a Be transparent with applicants on requirements for national security clearance holders

129. When an organisation advertises a position that requires a clearance, it SHOULD:

    a. inform potential applicants they will need to be vetted for a clearance, and to what level

    b. include an outline of the eligibility criteria or a link to the eligibility self-check tool, and

    c. encourage potential applicants to contact the organisation if they are unsure about their eligibility or the vetting process.

130. An organisation SHOULD make the ability to obtain and maintain a clearance a formal condition of employment where this is essential to an individual's role. An organisation SHOULD:

    a. notify potential applicants of this condition in the advertisement

    b. tell the preferred candidate before offering them employment or contract, and

    c. include the condition in the candidate's employment agreement (or a contract for services if they are a contractor or service provider).

131. An organisation SHOULD also apply this practice to new applicants, internal applicants, or secondment arrangements.

PERSEC 4.2.b Check eligibility for vetting

Check citizenship or visa status

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

133. In rare circumstances, an organisation may request vetting for a person who does not meet the eligibility criteria. The CSO MUST discuss the rare circumstances with the NZSIS Vetting Service first.

134. The organisation may then prepare a business case for vetting in rare circumstances. The organisation MUST first have NZSIS Vetting Service's agreement to draft the business case. The organisation's CE MUST approve the business case. Vetting may not proceed if the NZSIS Vetting Service does not accept the business case.

Make sure their background is checkable

135. Before an organisation initiates a vetting request, it MUST make sure each vetting applicant meets the minimum requirements for a checkable background.

136. In most cases, a person's background MUST be checkable for the immediately preceding required period of time or back to the age of 18. In some situations, it can be hard to assess whether a person meets the minimum requirements. The table below outlines the minimum checkable period for each clearance level.

Clearance Level	Background Checking
CONFIDENTIAL	5 years
SECRET	10 years
TOP SECRET	10 years
TOP SECRET SPECIAL	15 years

Where an applicant is too young to have a checkable background

137. If a vetting applicant does not have enough checkable years because of their age, an organisation may still submit a vetting request, and the NZSIS Vetting Service may recommend that a clearance is granted for a shorter time reflective of the number of checkable years for the applicant. For example, if the applicant is 20, they will only be checked back to the age of 18 even if the checkable background requirement is 5 years. The recommendation will be that an organisation only grant a clearance for 2 years.

Where an applicant has spent time living overseas

138. Time spent in Australia, Canada, the United Kingdom, and the United States of America is considered checkable. The NZSIS Vetting Service can let an organisation know whether they consider the applicant's background checkable or not if there are any concerns.

139. When applicants have worked overseas for a New Zealand Government organisation, their time in other countries can be checkable if that organisation gives assurance that they have managed the person in line with the Protective Security Requirements for clearance holders.

140. If recruiting from overseas, an organisation MUST ensure that the person still meets the minimum requirements for a checkable background.

PERSEC 4.2.c Check suitability for holding a clearance

141. Before an organisation submits a vetting request, it MUST have trust and confidence in the person and their ability to gain a favourable recommendation for a clearance by undertaking a review of records (such as performance or disciplinary records). Any

records that show dishonesty, misconduct, or breaches of the code of conduct are reviewed to ensure they are suitable to hold a clearance

142. An organisation MUST NOT initiate a vetting request if there are doubts that the applicant can be trusted with access to highly classified information, assets, or work locations.

143. If a risk assessment conducted by the organisation shows that it needs stricter criteria for deciding who to request vetting for, the organisation SHOULD apply those criteria alongside the mandatory eligibility and suitability requirements above.

PERSEC 4.2.d Request NZSIS vetting for a clearance

144. An organisation is responsible for submitting vetting requests for national security clearances to the NZSIS using Tiaki – the online security clearance management portal. An organisation MUST submit vetting requests to the NZSIS using Tiaki.

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

    b. The information applicants provide in their questionnaires can only be viewed by NZSIS Vetting Services staff.

    c. An organisation can check the progress of an application as it progresses through the vetting process, but they cannot access any information provided by the applicant or referees on their forms.

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

    a. overseas postings or deployments

    b. involvement in security-related court cases, or

    c. attendance at courses for which a clearance is required.

146. An organisation MUST contact the NZSIS Vetting Service to discuss an urgent vetting request before submitting it. If the NZSIS Vetting Service agree to the urgent request, include the following:

    a. a brief description of the circumstances that make the vetting urgent, and

    b. when a vetting recommendation by the NZSIS Vetting Service is needed by.

147. In an emergency, an organisation's CE may grant a person who already holds a clearance access to information, assets, or work locations classified one level above their current clearance. For more information about emergency access, see: PERSEC 4.4.d Manage emergency access to classified information, assets, or work locations.

PERSEC 4.2.e Decide whether to grant a clearance

148. When the NZSIS Vetting Service completes vetting the applicant for a national security clearance, they will give their written recommendation to an organisation's CSO (or delegate).

149. The NZSIS Vetting Service may recommend:

a. a clearance at the level requested

b. a clearance at a lower level than requested

c. a clearance with specific conditions ('qualifications') for managing the clearance, or

d. that a clearance should not be granted (not appropriate at any level).

150. The organisation MUST review the vetting recommendation from the NZSIS Vetting Service, which may include qualifications and decide whether to grant the clearance.

151. The organisation MUST inform the NZSIS of the organisation's decision.

152. The organisation MUST NOT grant a clearance at a higher level than the assessed level completed by the NZSIS Vetting Service. It may grant a clearance at a lower level.

153. When a clearance is granted, the organisation becomes the sponsor for the clearance. The organisation MUST assume responsibility for managing the clearance holder. This responsibility includes all other PERSEC4 requirements.

Vetting recommendation for the requested clearance level

154. If the NZSIS Vetting Service recommends a clearance at the level requested and the organisation decides to grant it, the organisation MUST provide the clearance holder with:

a. a briefing on their responsibilities to protect classified information, assets, and work locations

b. requirements for reporting any change in circumstances or suspicious contacts, and

c. details of the organisation's security awareness training programme

d. briefings from the NZSIS/GCSB relevant to any sensitive compartmented information they require access to

155. To help set expectations from the start, the organisation SHOULD inform new clearance holders that they will be evaluated regularly because their suitability to hold a clearance can change over time.

156. See Maintaining your national security clearance (PDF) for guidance outlining the responsibilities of a national security clearance holder to remain suitable to hold a clearance.

Vetting recommendation for a lower-level clearance

157. If the NZSIS Vetting Service has recommended a clearance at a lower level than the organisation requested, the organisation SHOULD:

a. advise human resources of the outcome of the vetting assessment if the clearance was a condition of employment, and

b. confirm the employment condition is met, or decide whether to withdraw the employment offer, redeploy the person, or terminate their employment.

Vetting recommendation with 'qualifications' on the clearance

158. When a vetting recommendation is received from the NZSIS Vetting Service with qualifications for security risk management, the organisation MUST establish a security risk management plan with the clearance holder.

159. If the organisation decides to grant a clearance to a foreign national, it MUST ensure the clearance holder is made aware of any additional responsibilities or restrictions that may apply to their clearance. For example, an organisation may make gaining New Zealand citizenship by a certain date a condition of maintaining their clearance.

Vetting recommendation that clearance not be granted

160. An organisation SHOULD NOT grant a clearance when they receive an adverse recommendation from the NZSIS about the applicant. The NZSIS Vetting Service should be contacted for more information.

PERSEC 4.2.f Advise vetting applicants about clearance decisions

161. A vetting applicant has the right to complain to the Inspector-General of Intelligence and Security (IGIS) if they are unhappy with:

    a. how the NZSIS carried out the vetting process, and/or

    b. the recommendation the NZSIS made.

162. Vetting applicants need to be made aware of their rights. The organisation MUST inform vetting applicants of their right to complain. Complaints must be made in writing. More information can be found at Complaints – Inspector-General of Intelligence and Security.

163. If an applicant complains, the organisation MUST wait until the IGIS complaint process is finished before taking any organisational action. Seek legal advice if needed.

164. See PERSEC Appendix C Procedural Fairness for more information on vetting candidates' rights and NZSIS' obligations to be thorough and fair in their assessment and recommendations.

PERSEC 4.3: Ensure the ongoing suitability of clearance holders

165. An organisation needs to consider personnel security throughout a national security clearance holder's employment or sponsorship. 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.

166. In addition to the requirements in PERSEC2, an organisation needs to support clearance holders to meet their responsibilities and ensure they remain suitable to hold a clearance. To meet these responsibilities, an organisation will:

    a. publish clear communications about personnel security for clearance holders

    b. provide security awareness training and updates

c. conduct security briefings when necessary

d. prepare clearance holders for international travel

e. ensure clearance holders report changes in their personal circumstances

f. ensure clearance holders report any suspicious contacts and behaviour

g. monitor and manage concerning behaviour, incidents, and changes in circumstances

h. manage emergency access to classified information, assets, and work locations

i. report changes to a clearance holder's security clearance level, and

j. regularly review and manage clearances.

PERSEC 4.3.a Provide security policies and practices for clearance holders

167. As part of GOV2 (Take a risk-based approach), an organisation MUST ensure clearance holders have access to clear policies and procedures that:

    a. explain security requirements for everyone as well as requirements specific to clearance holders, and

    b. outline all legal, regulatory, and compliance requirements.

168. The organisation MUST clearly communicate with the clearance holder to set the right expectations for their role. Ensure the clearance holder understands the organisation's security policies and practices and is aware of them when they change.

169. The organisation MUST ensure the clearance holder understands and acknowledges their specific responsibilities they have as a national security clearance holder.

170. The organisation SHOULD clarify with clearance holders if their continued employment is conditional on them maintaining a clearance to the appropriate level.

PERSEC 4.3.b Provide specific security awareness training for clearance holders

171. In addition to the requirements in GOV4 (Build security awareness), an organisation MUST provide security awareness training to clearance holders:

    a. at the time the clearance is granted, and

    b. at least every five years, as a condition for re-validating the clearance on renewal.

172. An organisation SHOULD provide updated security awareness training to clearance holders annually.

PERSEC 4.3.c Conduct security briefings for clearance holders

173. An organisation MUST conduct security briefings or debriefings with clearance holders when appropriate. The types of briefings that may be given to people when they start their role, or for specific purposes include:

a. overseas travel briefings, debriefings, and personal safety briefings when travelling on business or for personal purposes

b. briefings and debriefings for accessing TOP SECRET material

c. briefings and debriefings to allow access to specific protectively marked information or resources that have an endorsement, are compartmented or have codeword protection

d. briefings and debriefings for accessing highly classified material which is not normally accessed as part of their regular activity

e. specific location briefings for high-risk destinations or new facilities

f. briefings tailored for specific categories of employment, for example, the unique security issues for information technology (IT) staff, scientists and others

g. briefings tailored to contractors, temporary staff, and visitors

h. briefings tailored to the person's particular security needs as part of an ongoing security clearance management plan

i. risk management briefings in general, and protective security briefings in particular.

PERSEC 4.3.d Prepare clearance holders for international travel

174. New Zealand Government officials who travel overseas for work or personal reasons risk being targeted by foreign intelligence services with the capability and intent to target New Zealand interests.

175. Clearance holders may be even more at risk due to the nature of the information they may have access to. Clearance holders may be of interest to foreign intelligence services for several reasons, including New Zealand's:

a. position on international issues and agreements such as trade

b. strategic perspective and intentions on domestic policies

c. innovations in science and technology

d. economic or financial information

e. agriculture, primary industries, and other sectors that attract significant interest from foreign investors, and

f. defence and intelligence capabilities.

176. Clearance holders may be exposed to the same risks within New Zealand at conferences or while hosting international delegations.

177. An organisation MUST manage any risks with international travel. This includes having an overseas travel policy and process for managing travel requests and travel briefings.

178. The overseas travel policy MUST require clearance holders to:

a. consult the policy and security team to understand their security risks and obligations while travelling to mitigate the risks

b. discuss their travel plans before booking overseas travel (for personal and business reasons)

c. get formal permission from the organisation before finalising travel plans, and

d. obtain a travel briefing before travelling when deemed necessary by the security team.

179. If a clearance holder has received SCI briefings, the organisation MUST ensure that approval is obtained from GCSB for personal travel to specified countries.

180. To help prepare clearance holders for travel, organisations SHOULD provide them with the following guide: Advice for New Zealand Government officials travelling overseas for business (PDF).

181. An organisation COULD set restrictions on places clearance holders with SCIs can visit, airlines they can use, and activities that they can take part in.

PERSEC 4.3.e Ensure clearance holders report changes in personal circumstances

182. While the vetting process for a clearance gives an organisation a certain level of assurance about a person's suitability to hold a clearance, that assurance only applies to the time when vetting took place. It does not guarantee future suitability. Due to this, an organisation sponsoring clearances needs to:

a. review all security clearances to ensure the necessary level of assurance is maintained, and

b. check regularly to see if personal circumstances have changed for any clearance holder.

183. An organisation MUST require clearance holders to report any significant change in personal circumstances to the organisation as soon as they happen. The following changes in a clearance holder's circumstances are significant and must be reported:

a. starting or ending a close personal relationship

b. living in or visiting foreign countries

c. relatives living in foreign countries of security significance

d. changes in citizenship or nationality

e. changes in financial circumstances (for example, significant increases in wealth or debt)

f. changes in health or medical circumstances (for example, a serious medical condition could change a clearance holder's behaviour or cause financial difficulties, and prescription drugs can affect people's judgement)

g. involvement in criminal activity, accidentally or deliberately

h. involvement with any individual, group, society or organisation that may be of security concern

i. disciplinary procedures or security incidents that the organisation is involved in, and

j. any other changes in circumstance that may be of concern to the organisation.

184. When a significant change in circumstance is identified or reported, the organisation MUST conduct a risk assessment to determine whether the organisation needs to take further action (i.e. an individual security risk management plan)

185. If there are serious doubts about continuing the clearance that cannot be managed, the organisation SHOULD suspend or cancel the person's clearance until the risk is mitigated or assessed as no longer present. Refer to PERSEC Appendix B: Security Assessment Criteria and the Adjudicative Guidelines for risk assessment and mitigation guidelines.

186. For further guidance on assessing a clearance holder's continued suitability if a security incident, change in personal circumstances, or HR issue is reported, refer to PERSEC assessing changes in circumstances (PDF).

187. If the organisation is unsure whether a change in personal circumstances has implications for the holder's clearance, they may seek advice from the NZSIS Vetting Service.

Notify possible risks to national security

188. When a change of circumstance is considered especially significant or likely to present a risk to national security, the organisation MUST notify the NZSIS Vetting Service.

189. The NZSIS Vetting Service may require an organisation to initiate an out-of-cycle vetting assessment for the clearance holder, known as a 'review for cause'. See 4.4.b for more information.

190. If the NZSIS Vetting Service is satisfied that the clearance holder remains suitable to retain a clearance, then it will make a positive recommendation. The NZSIS Vetting Service's risk management advice may include specific measures the organisation MUST take.

PERSEC 4.3.f Conduct an annual security appraisal process

191. The organisation MUST conduct an annual security appraisal process with all clearance holders.

192. To support an organisation's regular review and management of the ongoing suitability of national security clearance holders, PSR provides example annual security appraisal form (ASAF) templates for organisational use. Refer to PSR PERSEC Resources for more information.

PERSEC 4.3.g Ensure clearance holders report concerns about other people

193. As part of GOV6 (Manage security incidents), an organisation MUST require and enable clearance holders to report concerning behaviours or incidents relating to people they work with as it could affect the individual's suitability to maintain a clearance and the security standards of an organisation. This includes:

    a. any significant changes in personal circumstances

    b. concerning behaviour, or

    c. security incidents.

PERSEC 4.3.h Ensure clearance holders report suspicious contacts

194. An organisation MUST require all clearance holders to report any suspicious contacts or requests to access their organisation's information, assets, or work locations to the organisation.

195. An organisation SHOULD ensure the clearance holders complete a contact report when an official or social contact appears suspicious, ongoing, persistent, or unusual (SOUP) in any respect. This contact could be with:

    a. embassy or foreign government officials within New Zealand,

    b. foreign officials or nationals outside New Zealand, including trade or business representatives, or

    c. 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'.

196. An organisation SHOULD have a clear process to assess all suspicious contact reports to determine whether it needs to:

    a. collect contact reports from other concerned people, and assess those reports

    b. advise the NZSIS of contacts that may have national security implications

    c. conduct an internal investigation (see GOV6, and/or

    d. notify relevant authorities for further investigation (for example, NZ Police, the Serious Fraud Office).

197. Sometimes a clearance holder's suspicious contacts may be of a criminal or business nature that involves a conflict of interest or gives a potential unfair advantage. An organisation SHOULD have a clear process to investigate these contacts and, if appropriate, notify appropriate authorities for further investigation.

PERSEC 4.3.i Ensure clearance holders minimise risks from social media use

198. When people share work or personal information on social media, criminals and foreign state actors may target them, using fake online profiles to try and gain access to valuable or sensitive information and resources.

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

200. Clearance holders need to be careful about what they post on social media, including work-related networks such as LinkedIn.

201. An organisation MUST ensure that clearance holders are informed on what they should and should not reveal, share, and use on social media (as defined within the organisation's policies and procedures) which may cover:

    a. Clearance holders must not post classified information or information about their own national security clearance.

    b. Clearance holders must avoid posting information about their work, unless it is for work purposes. Although posting unclassified information may not seem risky, it can have a big impact on security when it is combined with other information.

    c. Clearance holders should post as little personal information about themselves as possible. Consider carefully if clearance holders should reveal their:

        i. current or past employers

        ii. address

        iii. hobbies, likes, and interests

        iv. personally identifiable information, such as full date of birth

        v. compromising photos, and

        vi. location.

PERSEC 4.4: Manage security clearances

202. Managing a national security clearance holder 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.

PERSEC 4.4.a Monitor for concerning behaviour and incidents

203. Managers of clearance holders MUST monitor the clearance holder's behaviour for any security concerns, poor performance, or unacceptable conduct. Monitoring also involves watching for any signs that could suggest the person is unreliable or susceptible to pressure that could lead them to make poor security choices.

204. If a behavioural issue is identified, the organisation MUST support and manage the clearance holder through any resolution process.

205. An organisation MUST keep records of all clearance holders' security infringements, breaches and violations.

PERSEC 4.4.b Respond to security breaches

206. Concerns about the clearance holder can come from:

    a. the clearance holder

    b. the clearance holder's colleagues or supervisor/s, or

    c. any other person who reasonably believes the clearance holder's personal circumstances, attitude, or behaviour has changed.

207. If there is evidence that a clearance holder has breached security, an organisation's CSO (or delegate) MUST identify the response, which may include advising the NZSIS or the GCSB. Refer to GOV 6 for more information on security incident management. Possible responses may include:

    a. Providing the clearance holder with additional security awareness training.

    b. Initiating a 'review for cause'. A 'review for cause' is a review of a clearance holder when an organisation identifies security concerns that could affect their suitability to retain a clearance. The NZSIS carries out the review.

    c. Suspending access to classified information, assets, or work locations while undertaking a security incident investigation (which may include a review for cause).

    d. Regardless of any recommendation from a review for cause, the CE has the right to revoke a national security clearance if they no longer have confidence in the security clearance holder is appropriate to hold a clearance.

PERSEC 4.4.c Manage changes to security clearances

208. An organisation MUST actively use the NZSIS system Tiaki to manage and administrate clearances and the vetting process according to PERSEC 4 policy.

Review clearances after 5 years

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

210. The organisation MUST assign responsibility for managing the process to ensure the clearance continues, even if the clearance level changes.

Renew a clearance

211. To renew a clearance, an organisation MUST first determine the clearance holder's ongoing suitability to hold a clearance. If the clearance holder remains suitable, the organisation can then submit a security vetting renewal request to the NZSIS Vetting Service via Tiaki for their assessment. The renewal is initiated early enough to maintain continuity of the clearance.

212. The organisation MUST have trust and confidence in the clearance holder's ability to gain a favourable recommendation from the NZSIS Vetting Service before they submit a security vetting renewal request. To make such an assessment, the responsible

person MUST exercise their own judgement and view all the information available to them objectively.

Extend a clearance

213. An organisation may only grant an extension before a clearance expires and if there are no qualifications on the clearance.

214. An organisation may extend a clearance for up to 6 months at a time, up to a total of 12 months. The clearance MUST NOT be extended beyond a maximum of 12 months.

215. An organisation MUST complete due diligence to ensure the clearance holder is suitable for having their clearance extended.

216. If the clearance is shared with another organisation, the organisation MUST:

    a. review the sharing agreement before granting the extension

    b. notify the other organisation once the clearance has been extended.

Transfer a clearance

217. If a clearance holder is transferring directly to another organisation, their clearance may transfer with them. In general, an organisation may recognise a security clearance granted by another organisation if the correct transfer process has been followed.

218. 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:

    a. 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)

    b. there is a requirement to access classified information, assets, or work locations in the new role

    c. the transferred clearance is at the same level as the clearance originally recommended by the NZSIS

    d. 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), and

    e. The new organisation obtains from the clearance holder's former organisation:

        i. the vetting recommendation from the NZSIS, including any accompanying security risk management advice

        ii. written assurance of the clearance holder's continuing suitability to hold a clearance, and

        iii. notification of any relevant changes in the clearance holder's personal circumstance that happened after they were vetted.

219. SCI briefings do not automatically transfer with a security clearance. For further advice contact your organisation Communications Security Officer (COMSO) or CSO.

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

221. The transferring organisation MUST notify the NZSIS Vetting Service when the security clearance transfer has occurred as it will no longer be the sponsor.

222. The new organisation MUST ensure that the person has a clearance at or above the level required for the new role in the organisation.

223. The new organisation MUST NOT grant a clearance at a higher level without first receiving a vetting recommendation from the NZSIS Vetting Service.

Share a clearance

224. If an organisation is planning to work with, or second, a clearance holder sponsored by another organisation, it may be possible to share that clearance and for the two organisations to enter into joint sponsorship of the clearance. This situation may arise when a clearance holder's time is shared between organisations.

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

226. If there is an agreement to share a clearance, both organisations MUST:

    a. accept responsibility for sharing security concerns about the clearance holder

    b. agree on how the clearance will be managed and what each organisation will be responsible for

    c. inform each other about any changes in the clearance holder's circumstances, and

    d. ensure the clearance holder receives appropriate security briefings.

227. The original sponsoring organisation MUST:

    a. obtain permission from the clearance holder before sharing their personal information with the other organisation

    b. inform the other organisation if the last vetting recommendation for the clearance holder was routine

    c. share the last vetting recommendation with the other organisation if it was routine with information, qualified or adverse

    d. share any risk management plans in place for the clearance holder with the other organisation

    e. notify the NZSIS Vetting Service that a clearance will be shared and the organisation it will be shared with via Tiaki

    f. suspend or cancel the sharing agreement if a shared clearance has been suspended or cancelled

g. cancel the sharing agreement if a shared clearance ends

h. notify the other organisation if a shared clearance is downgraded, and

i. review and confirm that the sharing agreement is still acceptable if the clearance is transferred to another organisation.

Upgrade to a higher clearance level

228. If the tasks or duties of a role 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 need to undergo security vetting for that higher level.

229. To upgrade a clearance to a higher level, the sponsoring organisation MUST:

a. ensure that the holder is eligible to hold a clearance at the higher level

b. initiate a request to NZSIS Security Vetting Service to upgrade the clearance via Tiaki

c. grant the clearance once recommendation is received from the NZSIS

d. brief the holder on any new obligations associated with their higher clearance level, and

e. agree a plan for managing concerns or requirements in the NZSIS' vetting recommendation.

Downgrade to a lower clearance level

230. If a clearance holder moves to a new role that requires a lower level of clearance, and the person no longer requires the higher clearance, the sponsoring organisation SHOULD contact the NZSIS Vetting Service to downgrade the clearance. This could be a permanent or temporary move.

231. If it eventuates that the clearance holder needs to carry out duties at a higher clearance level, the organisation may allow them to if:

a. the initial vetting recommendation was at that higher level, and

b. the clearance is being managed appropriately and there are no security concerns.

PERSEC 4.4.d Manage emergency access to information, assets, or work locations that require a national security clearance

Approving emergency access

232. Sometimes an emergency may give rise to an urgent operational need for an existing clearance holder to access information, assets, or work locations above their clearance level.

233. Emergency access means an 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.

234. The CE of the sponsoring organisation or their delegate may grant a person emergency access. If the authority is delegated, it MUST be recorded in writing.

235. Emergency access MUST be:

    a. only to specified information, assets, or work locations required for the emergency

    b. only for the duration of the emergency

    c. governed by a very strict application of the need-to-know principle

    d. provided at no more than one level above a person's current clearance[1], and

    e. supervised by a manager with a suitable clearance.

236. Emergency access to SCI MUST be approved by the NZSIS and GCSB. For further advice contact your organisation COMSO or CSO.

Recording, briefing, and debriefing requirements

237. When granting emergency access, an organisation MUST:

    a. record that the emergency access has been granted

    b. brief the clearance holder appropriately

    c. ensure the clearance holder acknowledges they have been briefed them before being granted access and record this acknowledgement in writing

    d. debrief the clearance holder when the emergency ends.

Limits to using emergency access

238. An organisation MUST NOT use emergency access to allow a clearance holder access:

    a. for administrative or management purposes (such as helping them gain a position)

    b. when they are on reassigned duties while waiting for a security vetting recommendation (including a reclassification), and

    c. to classified information, assets, or work locations that carry an endorsement or compartmented marking.

239. An organisation MUST NOT grant emergency access to information, assets, or work locations marked CONFIDENTIAL or higher to anyone who does not hold a clearance.

PERSEC 4.5: Manage the clearance holder's departure

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

[1] 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.

241. When a person who holds a national security clearance leaves an organisation, the organisation MUST carry out the baseline PERSEC 3 activities and:

    a. conduct an exit interview

    b. transfer or cancel their security clearance

    c. debrief them from any SCI briefings they hold, unless the GCSB has given alternate advice, and

    d. update the clearance record via Tiaki.

PERSEC 4.5.a Remind the clearance holder of their ongoing obligations

242. The organisation MUST remind the clearance holder of:

    a. the need for their continued discretion after they leave the organisation, and

    b. their lifelong obligation to protect government information, assets, and work locations.

243. The organisation SHOULD obtain the clearance holder's written acknowledgement of these obligations.

PERSEC 4.5.b Cancel their security clearance

244. When a clearance holder leaves an organisation and the clearance is not being transferred, the organisation MUST cancel their clearance and notify the NZSIS Vetting Service that the clearance holder is no longer employed by that organisation.

PERSEC 4.5.c Debrief access from Sensitive Compartmented Information

245. Where the clearance holder had access to SCI, the organisation MUST ensure that a GCSB-authorised person:

    a. debriefs the clearance holder from any access to SCI

    b. conducts an exit appraisal with the clearance holder, and

    c. maintains post-separating contact with the departed clearance holder (if agreed).

246. For further advice contact SSU@gcsb.govt.nz