PERSONNEL SECURITY FOR GOVERNMENT AGENCIES

A GOOD PRACTICE GUIDE

Introduction

Personnel security practices provide agencies with a level of assurance about the honesty, trustworthiness and loyalty of individuals who access official information and assets. Appropriate personnel security allows agencies to deliver effective public services and reduces the risk of loss, damage or compromise of official information or assets.

All individuals working in the public service have access to official information and assets. Most do not require access to national security classified information, and therefore are not required to go through the security vetting process, but there are other personnel security measures agencies must implement to ensure an individual is suitable to have access to official information and assets.

The PSR establishes mandatory requirements for personnel security which apply to all agencies.

Mandatory requirement PERSEC1

Agencies must ensure New Zealand government employees, contractors and temporary staff who require ongoing access to New Zealand government information and resources:

- are eligible to have access
- have had their identity established
- are suitable to have access, and
- are willing to comply with government policies, standards, protocols and requirements that safeguard that agency’s resources (people, information and assets) from harm.

Agencies must have in place policies and procedures to assess and manage the ongoing suitability for employment of all staff and contractors.

This good practice guide is intended for agencies with staff who handle official information and assets but who do not require security vetting.
Personnel security measures

Measures for achieving a state of robust personnel assurance include the following.

Pre-employment checks – including confirming identity and right to work in New Zealand, checking references and any agency specific checks such as professional qualifications.

On-going personnel management – including briefings on employment conditions and codes of conduct, security training and education, and the promotion of a culture of security.

Separation activity – the agency and separating individual’s responsibilities including deeds of confidentiality and exit interviews.

Personnel security risk assessment – agencies must conduct risk assessments at the agency, group and individual level so that risks are identified, prioritised and treated appropriately.

The use of these measures:

- reduces the risk of loss, damage or compromise of official information or assets by providing assurance of the suitability of staff
- creates an environment where those with legitimate access to official information and assets are aware of their responsibilities and behave in accordance with standards of integrity and conduct published by the State Services Commission (SSC)
- minimises the potential for the misuse of official information and assets through deliberate or accidental disclosure
- encourages a positive security culture.

Personnel security risk assessment

Decisions about personnel security should be based on the agency’s personnel security risk assessment. The personnel security risk assessment should be integrated into the agency’s overarching protective security risk assessment as it may impact on, and should complement, information and physical security controls.

A security risk assessment will allow an agency to:

- identify and prioritise any employee risks
- identify appropriate countermeasures to mitigate risks
- allocate resources in a way that is cost effective, reflects the level of risk and complements other existing security controls
- highlight risks and proposed mitigations to senior management
- continually monitor the effectiveness of mitigation controls.

Agencies are recommended to undertake personnel security risk reviews every two years in accordance with:

Pre-employment checks

Agencies are expected to undertake pre-employment screening in accordance with the State Services Commission’s guidelines. These can be found on the Commission’s website at www.ssc.govt.nz/pre-employmentchecks.

SSC expects agencies to meet base level checks to confirm an individual’s identity in line with the Department of Internal Affair’s ‘Guidance on Establishing Identity in Recruitment Processes’. This can be accessed from the Evidence of Identity Standard section of DIA’s website at www.dia.govt.nz. In addition to the web page, there is a downloadable PDF with information and tools. It is recommended to human resources and security staff in all agencies.

Agencies are responsible for making sure applicants who are not New Zealand citizens have a legal right to work in New Zealand.

Factors which may individually, or in aggregate, raise serious concerns about an individual’s integrity – and therefore his or her suitability for employment – include:

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

Ongoing personnel management

People are an organisation’s strongest asset. Unfortunately they can also be its greatest weakness. An effective pre-employment screening policy will provide a reasonable degree of assurance an individual meets the required standards of trustworthiness, honesty and integrity at the time of the process. However, active and ongoing personnel security management is essential.

People and their behaviours are absolutely fundamental to good security. The easiest way to create a positive culture of security is through effective line management, personal responsibility and accountability.

While effective pre-employment screening will reduce the likelihood of recruiting problematic staff, people and their circumstances do change. This may happen over a period of time or suddenly as a reaction to a particular event.

The greatest risk to an agency is one posed by its own staff. This is often referred to as the ‘trusted insider’. A trusted insider is a person who exploits, or intends to exploit, their legitimate access to the employing agency’s resources for unauthorised purposes. The insider may be a permanent staff member or a contractor or secondee from another organisation. Studies1 have

1 The UK Centre for the Protection of National Infrastructure has released a report as part of an on-going programme of research into the insider threat. This is available on the CPNI website (www.cpni.gov.uk).
found the majority of insiders who breach security had no malicious intent when they started their employment. Instead they ‘go bad’ as a reaction to later events.

Common insider acts can include unauthorised disclosure of official, private or proprietary information, process corruption, unauthorised access to ICT systems, industrial espionage, theft and fraud. The insider’s motivation for this behaviour will vary and will often result from a combination of factors and pressures such as:

- revenge against an employer or colleagues in reaction to a real or imagined slight
- uncertainty regarding continued employment
- greed or financial gain
- political ideology
- ego or notoriety
- coercion, manipulation or exploitation from an external third party.

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

Effective countermeasures to insider threats include:

- management support – commitment to security from senior executives and the chief executive is vital as staff will model their behaviours
- communications – publishing clear policies and procedures explaining the rationale behind an agency’s security instructions, outlining legal, regulatory and compliance requirements, and ensuring staff understanding and accountability
- security awareness training – staff are much more likely to engage in the agency’s security culture if they understand the reason behind decisions and their own responsibilities in regard to them
- welfare – access to welfare facilities such as a confidential employee assistance programme will encourage staff to report and deal with personal issues before they become a serious problem
- managing behaviours of concern – agencies must provide managers with the tools and policies to identify, support and manage staff who display behaviours of security concern, poor performance or unacceptable conduct.

**Separation activity**

An employee who leaves an agency will retain knowledge of business operations, intellectual property, official information and security vulnerabilities. A formal exit procedure provides the opportunity to remind the departing employee of his or her obligations and can help to protect the agency and its resources.

An employee who leaves an organisation with a sense of disaffection is less likely to feel a sense of loyalty and may pose a greater risk. Managers should assess and manage any risk the departing employee may present. Depending on the level of risk, access to agency information, resources and premises may need to be restricted at an early stage of the separation process.

Exit interviews are a good opportunity to allow the affected individual to discuss their reasons for leaving and their attitude to the agency and remaining staff, and to surrender any passes or access cards they hold. It also allows the agency to remind the individual of their obligations to protect
information. A deed of confidentiality may be necessary to protect proprietary information or intellectual property.

Where there is any suspicion of malicious intent, the individual should be reminded of the provisions of the Protected Disclosures Act 2000. The Act is available at www.legislation.govt.nz.

In accordance with the values of the State Services Standards of Integrity and Conduct, agencies must provide honest and accurate references for separating staff.

**Further information**

The New Zealand government’s expectations for personnel security are similar to those of the United Kingdom. Further information and resources about personnel security can be found on the Centre for the Protection of National Infrastructure (CPNI) website at www.cpni.gov.uk.