GOV 1 Establish and maintain the right governance

GOV 1.1 Ensure executive commitment and oversight

a. Overall security accountability rests with the Organisation head
b. The Organisation head may delegate authority
c. Establish effective security governance oversight
d. Leaders promote and sponsor protective security

GOV 1.2 Assign functional security responsibilities

a. Appoint a Chief Security Officer (CSO)
b. Appoint a Chief Information Security Officer (CISO)
c. Ensure functional management and governance responsibility
d. Ensure security management is active and visible
e. Convene a Security Reference Group (SRG) when appropriate

GOV 2 Take a risk-based approach

GOV 2.1 Identify, assess, and manage security risks

a. Adopt an appropriate risk management approach
b. Identify and assess protective security risks
c. Consider risk measures when working or co-locating with others
d. Manage your security risks effectively

GOV 2.2 Formulate security plans

a. Ensure security plans addresses key risks
b. Regularly review, update, and phase security actions

GOV 2.3 Define and articulate security policies, processes, and procedures

a. Develop security policies
b. Define security processes, procedures, and guidance
c. Review your security policies and processes

PSR | Protective Security Requirements

GOV 3 Prepare for business continuity

GOV 3.1 Set the scope of the business continuity programme

a. Develop a policy for managing business continuity
b. Assign responsibility for business continuity

GOV 3.2 Identify critical functions and their requirements

a. Identify critical functions
b. Conduct a business impact analysis

GOV 3.3 Develop solutions and plans for maintaining critical functions

a. Develop solutions
b. Document business continuity planning and procedures
c. Establish teams to manage business continuity in a disruption

GOV 3.4 Monitor the level of preparedness for a disruptive event

a. Educate people on your business continuity arrangements
b. Run exercises to validate business continuity plan and prepare for disruptions

GOV 3.5 Review and maintain the business continuity programme

a. Review plans regularly to ensure effectiveness and continual improvement
b. Maintain your business continuity programme

GOV 4 Build security awareness

GOV 4.1 Establish a security awareness and training programme

a. Set the scope of your security awareness and training programme
b. Set security awareness programme goals

GOV 4.2 Implement security awareness training

a. Ensure security awareness is an ongoing and regular part of operations
b. Provide additional training for people in emergency, safety, or security roles
c. Train personnel on how to protect assets
d. Provide guidance on upholding legislation for protecting official information
e. Train personnel to report security concerns

GOV 4.3 Build a strong security culture

a. Communicate effectively to enhance your security culture
b. Monitor training effectiveness
c. Monitor security behaviours and culture
d. Manage poor security behaviour effectively

GOV 5 Manage risks when working with others

GOV 5.1 Understand the risks from your supply chain

a. Principle 1: Understand what needs to be protected and why
b. Principle 2: Know who your suppliers are and understand their security measures
c. Principle 3: Understand the security risks posed by your supply chain

GOV 5.2 Establish effective control and oversight of your supply chain

a. Principle 4: Communicate your view of security needs to your suppliers
b. Principle 5: Set and communication minimum security requirements for your suppliers
c. Principle 6: Build security considerations in contracting process and require suppliers to do the same
d. Principle 7: Meet your own security responsibilities as a consumer
e. Principle 8: Raise awareness of security within your supply chain
f. Principle 9: Provide support for security incidents

GOV 5.3 Check you supply chain arrangements

a. Principle 10: Build assurance activities into supply chain management

GOV 5.4 Continuous improvement

a. Principle 11: Encourage the continuous improvement of security within your supply chain
b. Principle 12: Build trust with suppliers

GOV 6 Manage security incidents

GOV 6.1 Establish an effective approach to managing security incidents

a. Follow a structured approach for security incident management
b. Establish policies and procedures for managing security incidents
c. Prepare and test your incident response readiness

GOV 6.2 Ensure that security incidents are detected and raised

a. Require personnel to raise security incidents and make it easy for them to do so
b. Establish mechanisms to quickly detect and respond to security incidents

GOV 6.3 Record and assess security incidents

a. Implement methods for recording and assessing the impact of security incidents

GOV 6.4 Report security incidents to relevant agencies

a. Report certain security incidents to other agencies
b. Report security incidents involving holders of national security clearances
c. Report cyber security incidents to the National Cyber Security Centre
d. Report security incidents involving Cabinet material to the Cabinet Office
e. Report criminal incidents to law enforcement bodies
f. Include these details when you report major security incidents

GOV 6.5 Investigate, respond to, and manage security incidents

a. Investigate security incidents
b. Take interim measures while investigations are underway
c. When appropriate, involve others in security investigations

GOV 6.6 Learn from security incidents

a. Monitor and measures incident management effectiveness
b. Conduct post-incident reviews when appropriate
c. Research incident management practice practices and security trends

GOV 7 Be able to respond to increased threat levels

GOV 7.1 Identify sources of risk for heighted security alert levels

a. Use internal and external sources of information to inform response planning

GOV 7.2 Develop alert levels

a. Establish alert levels that address all types of emergency and security alerts

GOV 7.3 Plan your response during heightened security alerts

a. Determine your security measures at different alert levels
b. Develop a plan for changing security alert levels

GOV 7.4 Monitor the risk environment and change alert levels when necessary

a. Change alert levels when necessary
b. Debrief after changing alert levels

GOV 7.5 Review and update your processes

a. Practice, review, and improve alert response processes

GOV 8 Assess your capability

GOV 8.1 Monitor and measure your protective security performance

GOV 8.2 Assess your protective security capability

GOV 8.3 Set your protective security goals for improvement

GOV 8.4 Provide assurance of your protective security capability and goals

GOV 8.5 Report on your protective security capability and improvement plans

INFOSEC 1 Understand what you need to protect

INFOSEC 1.1 Understand the value of your information

a. Create an inventory of information and ICT systems
b. Assess the impact of possible information security incidents

INFOSEC 1.2 Assess the risks to information security

INFOSEC 2 Design your security measures

INFOSEC 2.1 Adopt an appropriate information security management framework

INFOSEC 2.2 Design and implement information security measures

a. Use appropriate information security design approaches
b. Implement appropriate access controls
c. Address the points where your information could face critical risks

INFOSEC 2.3 Follow the Classification System

a. Adopt Classification System principles
b. Classify and assign protective markings
c. Protect classified information
d. Handle government information securely

INFOSEC 3 Validate your security measures

INFOSEC 3.1 Ensure appropriate certification and accreditation

INFOSEC 4 Keep your security up to date

INFOSEC 4.1 Analyse evolving security vulnerabilities and threats

a. Monitor for security events and vulnerabilities
b. Monitor evolving threats to information security

INFOSEC 4.2 Keep Information security measures up to date

INFOSEC 4.3 Respond to information security incidents

INFOSEC 4.4 Review security measures

a. Conduct periodic reviews and assure compliance
b. Identify changes required to organisational information security

INFOSEC 4.5 Retire information securely

PHYSEC 1 Understand what you need to protect

PHYSEC 1.1 Identify what you need to protect

a. Understand how your facilities and work locations are used
b. Assess the impact of security breach

PHYSEC 1.2 Assess physical security risks

a. Assess the risks of each site
b. Assess risks when selecting new sites

PHYSEC 2 Design your security measures

PHYSEC 2.1 Apply good practices for physical security design

a. Identify physical security measures needed to address your risks
b. Consider physical security design early
c. Use security zones to reflect business impact levels
d. Consider using multiple layers of security
e. Apply other good practices in physical security design

PHYSEC 2.2 Develop security plans

a. Prepare site security plans

PHYSEC 2.3 Implement specific physical security measures

a. Use NZSIS approved products
b. Implement the specific physical security measures required for each site
c. Manage specific scenarios
d. Build physical security into your business relationships and contracts
e. Maintain records

PHYSEC 3 Validate your security measures

PHYSEC 3.1 Ensure security zones are certified and accredited

PHYSEC 4 Keep your security up to date

PHYSEC 4.1 Analyse security vulnerabilities and threats

PHYSEC 4.2 Keep physical security measures up to date

PHYSEC 4.3 Respond to physical security incidents

PHYSEC 4.4 Review security measures

PHYSEC 4.5 Retire securely

PERSEC 1 Recruit the right person

PERSEC 1.1 Carry out baseline checks for all roles

a. Confirm identify and nationality
b. Confirm the right to work in New Zealand
c. Check references with former employers
d. Conduct a criminal record check

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

a. Psychometric testing
b. Checks of qualifications and/or occupational registrations
c. Credit checks
d. New Zealand Police check
e. Drug and alcohol checks

PERSEC 1.3 Address any concerns from pre-employment checks

a. Create a risk management plan if necessary
b. Record what is discovered

PERSEC 1.4 Set the right expectations

PERSEC 2 Ensure their ongoing suitability

PERSEC 2.1 Carry out minimum requirements to ensure ongoing suitability

PERSEC 2.2 Carry out ongoing suitability checks for higher risk roles

a. Ensure significant changes in personal circumstances are reported
b. Ensure suspicious contacts are reported
c. Brief people on the risks related to international travel

PERSEC 2.3 Manage role changes

a. Undertake appropriate checks on personnel changing roles

PERSEC 2.4 Manage contractors

PERSEC 3 Manage their departure

PERSEC 3.1 Remove access and collect assets

PERSEC 3.2 Conduct debriefs and confidentiality agreements

PERSEC 4 Manage national security clearances

PERSEC 4.1 Determine the clearance level needed

a. Considerations for determining the required clearance level
b. Considerations for access to classified and sensitive compartmented information
c. Considerations for short term or temporary access

PERSEC 4.2 Determine eligibility and suitability for a national security clearance

a. Be transparent with applicants on requirements for a national security clearance
b. Check eligibility for vetting
c. Check suitability for holding a clearance
d. Request NZSIS vetting for a clearance
e. Decide whether to grant a clearance
f. Advise vetting applicants about clearance decisions

PERSEC 4.3 Ensure the ongoing suitability of clearance holders

a. Provide security policies and practices for clearance holders
b. Provide specific security awareness training for clearance holders
c. Conduct security briefings for clearance holders
d. Prepare clearance holders for international travel
e. Ensure clearance holders report changes in personal circumstances
f. Conduct an annual security appraisal process
g. Ensure clearance holders report concerns about other people
h. Ensure clearance holders report suspicious contacts
i. Ensure clearance holders minimise risks from social media use

PERSEC 4.4 Manage security clearances

a. Monitor for concerning behaviour and incidents
b. Respond to security breaches
c. Manage changes to security clearances
d. Manage emergency access to classified information, assets, or work locations

PERSEC 4.5 Manage the clearance holder's departure

a. Remind the clearance holder of their ongoing obligations
b. Cancel their security clearance
c. Debrief access from sensitive compartmented information