PSR | Protective Security Requirements

COMPLIANCE GUIDE

This guide provides a simple checklist to help agency security leaders to review their organisation's security capability. It is based on the mandatory requirements of the Protective Security Requirements and also best practice.

This guide is a general and introductory resource. It does not span the full range of security issues and risks that individual agencies will need to consider.

Security Governance

1	Are you and your security staff familiar with the Protective Security Requirements and the New Zealand Information Security Manual?	Yes	No
2	Do you have an agency Chief Security Officer?	Yes	No
3	Do you have documented security policies, a security plan, and security processes and procedures?	Yes	No
4	Are these updated at least every two years, or sooner if needs dictate?	Yes	No
5	Have you conducted a security threat and risk analysis for your organisation?	Yes	No
6	Do you have a security risk register?	Yes	No
7	Have you prioritised your risks and are you applying mitigations?	Yes	No
8	Does the CSO meet at least quarterly with the agency head to discuss security?	Yes	No
9	Does the CSO meet at least quarterly with staff with security responsibilities, to discuss and coordinate security as a group?	Yes	No
10	Do you have effective procedures for reporting security incidents and suspicious activity?	Yes	No
11	Do you have a staff security awareness campaign?	Yes	No
12	Do you undertake an annual security assessment?	Yes	No
13	Does your agency have a business continuity management plan in place that considers security issues?	Yes	No

Personnel Security

1	Do you conduct appropriate checks, based on role and access, on all personnel before engaging them and allowing them to access government-held information and resources?	Yes	No
2	Do you have processes in place to assess the continuing / ongoing suitability of all personnel to access government-held information and resources?	Yes	No
3	Do you ensure that *only* those staff who *need* a clearance have their clearance processed and that it is *only* processed to the *level* of clearance required?	Yes	No
4	Do you maintain a register of all personnel and contractors who have been granted a security clearance by your organisation?	Yes	No
5	Do you advise the NZSIS when a clearance is granted, cancelled, downgraded, suspended, or when a security cleared staff member leaves the organisation?	Yes	No
6	Are position descriptions reviewed to check the level of clearance required (if any)?	Yes	No
7	Do you brief staff (including employees, contractors and temporary staff) on their responsibilities and obligations when a clearance is granted?	Yes	No
8	Are cleared staff aware of the need to report changes in personal circumstances and what constitutes a change of circumstances?	Yes	No
9	Do cleared staff report intended overseas travel?	Yes	No
10	Do cleared staff travelling to countries of security concern receive a travel briefing detailing potential risks?	Yes	No
11	Do managers monitor staff and include security in annual performance appraisals?	Yes	No
12	Does your staff induction programme include security training?	Yes	No
13	Are disciplinary matters cross-referenced to security records?	Yes	No
14	Do you have a system that allows staff to report any unusual or suspicious contact that they have experienced? This could be foreign contact, or someone attempting to obtain official information they don't have a valid need-to-know.	Yes	No
15	Are exit debriefs and interviews conducted with cleared staff on their departure?	Yes	No
16	Are all employees, contractors and temporary staff required to sign a confidentiality (non-disclosure) agreement when working in sensitive information areas?	Yes	No
17	Do your contracted service providers comply with the requirements of the PSR when delivering services to you?	Yes	No
18	Do you ensure you always receive a recommendation from the New Zealand Security Intelligence Service before granting a national security clearance?	Yes	No
19	Are all visitors escorted when around sensitive areas?	Yes	No

Information Security

1	Do you have clear policy and framework that address information security and management requirements?	Yes	No
2	Have you documented and implemented operational procedures and measures surrounding the protection of your information and systems, including in accordance with the New Zealand Information Security Manual?	Yes	No
3	Do you ensure that relevant elements of the above are clearly communicated to staff?	Yes	No
4	Are your rules surrounding control of access consistent with business requirements, information classifications and legal obligations?	Yes	No
5	Do your security measures for all information management processes and ICT systems adhere to any legislative or regulatory obligations under which you operate?	Yes	No
6	Do you have measures in place to protect and control protectively marked information in both electronic and paper-based formats?	Yes	No
7	Are protectively marked information and systems only accessible by staff with a suitable clearance?	Yes	No
8	Do staff routinely practice a clear desk policy ensuring protectively marked materials are not left unattended?	Yes	No

Physical Security

1	Do you have a clearly communicated policy that meets the PSR requirements and guidance relating to physical security?	Yes	No
2	Do you have adequate physical access controls (e.g. swipe cards, keys, locks, alarms systems, wearing of ID, CCTV)?	Yes	No
3	Are your secure or restricted areas only accessible by staff with a suitable clearance?	Yes	No
4	Are locks and storage devices appropriate for the classification level of the information stored within them?	Yes	No
5	Are your intruder detection systems and alarms approved, maintained and tested?	Yes	No
6	Do you restrict the use of electronic devices at sensitive meetings, i.e. leave them outside the meeting?	Yes	No
7	Are your physical security measures consistent with relevant occupational health and safety obligations?	Yes	No
8	Are you able to regulate/remove the risk of information and ICT equipment being made inoperable or inaccessible, or being accessed without proper authorisation?	Yes	No
9	Have you developed plans and procedures to move to heightened levels of security in case of emergencies and increased threats?	Yes	No
10	Do you have appropriate security features in place to ensure the physical wellbeing of staff and visitors?	Yes	No

Based on the above, we need to focus on: