PSR | Protective Security Requirements

Policy Version: 1.0 ***Last Review Date: July 2025***

Protective Security Requirements (PSR) Policy Framework:

PSR Glossary of Terms

PSR Glossary of Terms

Term	Definition
Access	Obtaining knowledge or possession of information (including verbal, electronic and hard copy information) or other resources, or obtaining admittance to an area.
Access control system	A system designed to limit access to facilities or systems to authorized people whose identity has been verified.
Accountable material	Accountable material is information that requires the strictest control over its access and movement, as well as regular auditing, to ensure its safe custody.
Accreditation	The process by which an approving authority gives formal recognition and approval that appropriate levels of security have been implemented to protect facilities and/or systems. Accreditation is designed to ensure minimum standards are met and maintained throughout the lifespan of facilities and Information and Communications Technology (ICT) systems, and that any residual risks are appropriately managed.
Accreditation authority	The person and organisation responsible for approving accreditation of a facility or ICT system. See NZISM for ICT system accreditation authority requirements and PSR PHYSEC for facilities accreditation authority requirements.
Aggregation	A term used to describe collections of protectively marked or UNCLASSIFIED official information or assets where the business impact from the compromise of confidentiality, loss of integrity or unavailability of the combination of the information or assets is greater than its component parts and may require a higher level of protection.
Agreement (information sharing)	An instrument, agreement or treaty between the New Zealand Government and another government. An arrangement or Memorandum of Understanding (MOU) between a New Zealand government agency and a foreign agency for the exchange and protection of information.
Asset	An item that has a value to an organisation – including personnel, information, physical assets and services. Also see Official resources.
Audit	An independent examination and verification of an agency's systems and procedures, measured against predetermined standards.
Authentication	The process of confirming a claimed identity or information.
Availability	Availability means that authorised users have access to the information that they need. See also Integrity and Confidentiality.
Bilateral agreement	An agreement between the New Zealand government or a New Zealand government agency and the government or agency of another country that provides for the reciprocal exchange of official information. Also see Multilateral agreement and Foreign Government Information (FGI).

Term	Definition
Breach	See security breach.
Briefings	Additional specific training required before a person is given access to certain compartmented marking information or sensitive sites.
Business Impact Level (BIL)	The level of impact on an agency's ability to operate or on the national interest, resulting from the compromise of confidentiality, loss of integrity or loss of availability of people, information or assets.
Certification	A procedure by which a formal assurance statement is given that functions, goods or services conform to a specified standard.
CISO	Chief Information Security Officer (CISO). A senior executive who is responsible for coordinating communication between security and business functions. The CISO also oversees the application of controls and security risk management processes within an agency.
CSO	Chief Security Officer (CSO). The CSO is an agency executive with overall responsibility for security. The CSO is answerable to, and must have free access to, the agency head on all security-related matters.
Classification System	New Zealand Government Information Security Classification System. This is New Zealand government's administrative system (principles, policies, guidance, tools, and resources) for the appropriate classification and handling of government information to ensure it is appropriately used, managed, and protected.
Classified information	Classified information is any government information that requires security and special handling to protect it. The information is generally protectively marked with the classification level (e.g. IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET) and may also include other endorsement or compartmented markings. See also Protective marking, Endorsement marking, and Compartmented marking.
Clear desk policy	A policy requiring an individual to ensure that protectively marked or UNCLASSIFIED official information and other valuable resources are secured appropriately when the person is absent from the workplace.
Clear screen policy	A supplementary policy to the clear desk policy that requires a person to ensure that information on ICT equipment is secured appropriately when the person is absent from the work station, for example, by locking the ICT equipment.
CMM	Capability Maturity Model. PSR has developed the PS-CMM model and guidance. NCSC has developed the CS-CMM model.
Codeword	A type of compartmented marking. A codeword indicates that the information it covers is in a special need-to-know category. Those with a need to access the information will be cleared and briefed about the significance of this type of information.

Term	Definition
Compartmented marking	A compartmented marking is an additional protective marking that is combined with the classification and endorsement marking (if applicable) indicating that the information is in a specific compartment. This word could be a codeword or 'Sensitive Compartmented Information (SCI)'. See also Protective marking, Need-to-know', Endorsement marking, and SCI.
Compromise	Compromise is the intentional or unintentional unauthorised disclosure, removal, tampering, destruction, or misuse of information/assets.
Confidentiality	Confidentiality means that information is protected from unauthorised disclosure or access. See also Integrity and Availability.
Control	A measure used to protect from compromise of confidentiality, integrity and availability, or mitigate an identified threat to an organisation's people, information or assets.
Countermeasures	Barriers, including procedural, logical or physical countermeasures, used to protect official resources.
Decision-useful information	Information is decision-useful when it assists users to make good decisions or informs the development of advice to decision-makers. To be decision-useful, the information needs to be high-quality, timely, and accurate.
Declassification	Declassification is the process for reviewing the protective marking on information with the objective of removing or downgrading classifications to facilitate the public release of information.
Delegate	A person authorised by another person to act on their behalf. In most cases, a delegate is a senior person authorised to act on an organisation head's behalf.
Disposal	In the context of information and records, disposal means the decision-making processes for retaining, transferring or destroying information and records.
Double enveloping	The use of two unused opaque envelopes (an inner and an outer envelope) to help protect protectively marked information in transit from unauthorised access and, in the event of unauthorised access, provide evidence of this to the recipient.
Electronic information	Data or information stored or generated electronically including metadata.
Emergency access	Supervised access to protectively marked material one level above an individual's current security clearance, when there is an urgent and critical operational need to do so.
Encryption	The process of transforming data into an unintelligible form to enable secure transmission.

Term	Definition
Endorsement marking	An endorsement marking is an additional protective marking that combined with the classification, warn people that information has special handling requirements. The endorsement marking may indicate the specific nature of information, temporary sensitivities, limitations on availability, or conditions for handling. See also Protective marking and compartmented marking.
Exposure	The degree to which a resource is open to, or attracts, harm.
Facility	A building, part of a building or complex of buildings, in which an agency, or a particular agency function, is located. This can include contractors' premises and home offices.
Firewall	A programme or device designed to prevent unauthorised access to or from a network or system by filtering incoming and outgoing network data based on a series of rules.
Foreign government	Any government external to New Zealand (including an individual, organisation or agency acting on behalf of this government) or an intergovernmental organisation. This also includes multi-national or supra-national government and non-governmental organisations, for example, the Asia-Pacific Economic Cooperation, North Atlantic Treaty Organisation, European Union, United Nations and Interpol.
Foreign Government Information (FGI)	Information received by the New Zealand government from foreign governments and government agencies in support of strategic and operational objectives. In most cases, New Zealand provides the assurance to safeguard this information under the terms of a bilateral and multilateral agreement, Security of Information Agreement or Arrangement (SIA) or MOUs.
GCDO	Government Chief Digital Officer (GCDO). As system leader for government ICT, the GCDO (previously called the Government Chief Information Officer GCIO) is responsible for ICT-enabled transformation across government agencies to deliver better services to citizens.
GCISO	The Government Chief Information Security Officer (GCISO) is a system leadership role appointed by the Public Service Commissioner to the Director-General of the Government Communication Security Bureau (GCSB).
GCSB	Government Communications Security Bureau (GCSB). The GCSB ensures the integrity and confidentiality of government information, and investigates and analyses cyber incidents against New Zealand's critical infrastructure. The GCSB also collects foreign intelligence bearing on New Zealand's interests, and assists other New Zealand government agencies to discharge their legislatively mandated functions.

Term	Definition
Government information	Government information is all information, regardless of form or format, from documents through to data, that the New Zealand government collects, stores, processes, generates, or shares to deliver services and conduct business. This includes information from or exchanged with the public, external partners, contractors, or consultants and includes public records, email, metadata, and datasets.
GPSL	The Government Protective Security Lead (GPSL) is a leadership role appointed by the Public Service Commissioner to the Director-General of the New Zealand Security Intelligence Service (NZSIS).
Harm	Any negative consequence, such as the compromise of, damage to, or loss of, people, assets, or information.
Hazard	A source of potential harm – a hazard might include a threat.
ICT	Information and Communications Technology (ICT). Describes any device or application used to communicate, record, process, store and/or transfer information, including data storage devices, mobile telephones and mp3 players, and the operating systems, hardware and software applications used to operate networks and systems.
ICT equipment	Any device that can process, store or communicate electronic information, for example, computers, multi-function devices and copiers, landline and mobile phones, digital cameras, electronic storage media and other radio devices.
ICT facility	A building, floor of a building or designated space on the floor of a building used to house or process large quantities of data, for example, server and gateway rooms, data centres, back-up repositories, storage areas for ICT equipment and communications and patch rooms.
ICT system	A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.
INFOSEC	Information Security (INFOSEC). The application of security controls to information systems that are commensurate with the protective marking, sensitivity and/or value of that information and compliant with government policy.
Information, information assets or information resources	Documents and papers, electronic data, the software or systems and networks on which the information is stored, processed or communicated, intellectual information acquired by individuals and physical items from which information regarding design, components or use could be derived that add value to an organisation.
Inherent risk	The raw or untreated risk. See also Protective Security Threat and Risk Guidance. See also Residual risk.

Term	Definition
Insider Threat	Any person who exploits, or intends to exploit, their legitimate access to an agency's assets to harm the security of their agency or New Zealand, either wittingly or unwittingly, through espionage, terrorism, unauthorised disclosure of information, or loss or degradation of a resource or capability.
Integrity	Integrity means that information is protected from unauthorised changes to ensure it remains reliable and correct. See also Availability and Confidentiality.
Malware	Malicious software. Software designed to disrupt computer operation, gather sensitive information or gain unauthorised access to computer systems.
MFDs	Multi-function devices.
MCSS	Minimum Cyber Security Standards. Standards developed by the New Zealand Cyber Security Centre.
Mobile computing	Work from a non-fixed location using portable computing and/or communications devices, for example, laptops, notebooks, tablets, smart mobile phones and personal digital assistants.
Multilateral agreement	An agreement between the New Zealand government, or a New Zealand government agency, and the government, or agencies, of multiple countries that provides for the reciprocal exchange of official information. Also see Bilateral agreement and Foreign Government Information.
National interest	National interest means the maintenance of New Zealand's good international reputation and bilateral relations, public confidence in the areas of tourism, trade, the economy and government, and the security and safety of all New Zealanders.
National security	A term used to describe the safety of the nation from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on New Zealand's defence system, acts of foreign interference or serious organised crime, as well as the protection of New Zealand's borders.
National Security Clearance	A New Zealand government national security clearance is a status held by individuals deemed eligible and suitable to access official information classified at C*NFIDENTIAL and above. The individual must meet the minimum criteria and checkable background period for the national security clearance required, and undergo security vetting by the NZSIS. National security clearances are role-based and must be sponsored by a government organisation.
National security information	Official information that, if compromised, could affect the security of the nation. National security information could include information about protection from espionage, sabotage or politically motivated violence.
NCSC	National Cyber Security Centre (NCSC) is part of GCSB responsible for enabling the protection, wellbeing, and prosperity of Aotearoa New Zealand b providing trusted cyber security services.

Term	Definition
NZISM	New Zealand Information Security Manual. The Government's manual on information assurance and information system security.
NZSIS	New Zealand Security Intelligence Service (NZSIS) The NZSIS establishes personnel and physical security standards for the protection of national security information, as authorised by The Intelligence and Security Act 2017. The NZSIS is responsible for providing advice to the New Zealand government relating to New Zealand's security.
Need-to-go	Access to an area should be limited to those who require access to do their work, for example, cleaners – they do not have a need to know but they do have a need to go to do their work.
Need-to-know	The principle that a user must have a legitimate reason to access and use information or equipment to meet an operational need.
Need-to-share	The principle that government information needs to be appropriately shared to enable the protection of New Zealand and New Zealanders from threats, and to realise the potential of information to aid government effectiveness and enable wellbeing of New Zealanders.
Official information	A subset of Government information (see Government information). Any information generated, received, developed, or collected by, or on behalf of, the New Zealand government through its agencies and external service providers that is not publicly available, including sensitive information and protectively marked information, such as: - documents and papers - data - the software or systems and networks on which the information is stored, processed or communicated - the intellectual information (knowledge) acquired by individuals - physical items from which information regarding design, components or use could be derived. See the Official Information Act 1982.
Official resources	Includes official information, people who work for, or with, the New Zealand government, and assets belonging to, or in the possession of, the New Zealand government. Official resources include resources belonging to the New Zealand government but in the possession of contractors.
Open information	Open information is unclassified information that has been made available to the public for their use and sharing. See also Unclassified information.
Organisation head	The head of an organisation. Endorses and is accountable for all protective security within the organisation.

Term	Definition
Originator (of information)	The person, or agency, responsible for preparing or creating official information or for actioning information generated outside the New Zealand government. This person, or agency, is also responsible for deciding whether, and at what level, to protectively mark that information.
Paragraph marking	Paragraph marking is the practice of marking the classification level of a section of information within a document, email, or dataset. This informs the user of which sections contain the information of the highest classification and enables more appropriate sharing of information.
Partner	Refers to any individuals, groups, organisations, or governments where information is shared.
PERSEC	Personnel Security (PERSEC). The management of personnel to assist in the protection of an agency's people, information and assets. It includes the screening and ongoing education and evaluation of employees.
Personal information	Information or an opinion (including information forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. For further details, see the Privacy Act 2020.
Personnel	Any member of an agency's staff (ongoing and non-ongoing), contracted service providers requiring access to protectively marked information or resources, or other people who provide services to the agency or access agency information or assets.
Physical asset	An item of economic, commercial or exchange value that has a tangible or material existence, including assets (for example, computers) that contain official information.
PHYSEC	Physical security (PHYSEC). The part of protective security concerned with the provision and maintenance of a safe and secure environment for the protection of agency employees and clients as well as physical measures designed to prevent unauthorised access to official resources and to detect and respond to intruders.
Privacy	A person's ability to control the availability of information about them.
Protective marking	Protective marking is the practice of marking the information with its classification, endorsement markings, and compartmented markings (if applicable) such as within paragraphs, emails, documents, metadata, or systems to inform readers and users of their obligations for securely handling and protecting the information.
PSR	Protective Security Requirements (PSR) outlines the Government's requirements for managing personnel, physical, and information security. The Classification System is a core foundation to the PSR. The PSR was approved by Cabinet in 2014 [CAB (14) 39/38]
PSR Assurance Framework	Framework to enable organisations to select, establish, assess, and assure that they have appropriate levels of protective security capability to address their level of risk.

Term	Definition
Removable media	Storage media that is easily removed from a system, designed for removal and is not an integral part of the infrastructure. For example, magnetic tapes, CDs or DVDs, USBs, microfilms and removable hard drives.
Residual risk	The level of risk remaining after mitigations are applied. See also Inherent risk.
Risk	The chance of something happening that will materially impact the achievement of objectives – it is measured in terms of event likelihood and consequence.
Risk acceptance	An informed decision to accept a risk within the context of any mitigations applied.
Risk analysis	The systematic process to understand the nature, and to deduce the level, of risk. This includes identification and evaluation.
Risk appetite	Statements that communicate the expectations of an agency's senior management about the agency's risk tolerance. These criteria help an agency identify risk and prepare appropriate treatments and provide a benchmark against which the success of mitigations can be measured.
Risk avoidance	A decision not to become involved in a risk situation, for instance, through deciding not to start or continue the activity that gives rise to the risk.
Risk management	Coordinated activities to direct and control an organisation with regard to risk.
Risk mitigation	Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk.
Risk rating	A rating that indicates how significant each identified potential risk is to an agency. The risk rating may be expressed qualitatively or quantitatively, based on the risk likelihood and consequence.
Risk time horizon	The proximity of when the risk might eventuate. Knowledge of the time horizon, or time to impact should the risk occur, contributes to the risk mitigation decision making.
Risk transfer	Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means.
Safe hand	A method of transporting an article in such a way that the article is in the care of an authorised officer or a succession of authorised officers who are responsible for its carriage and safekeeping. The purpose of sending an article using safe hand is to establish an audit trail that allows the sender to receive confirmation that the addressee received the information.
Sanitation	The process of removing certain elements of information that will allow the protective marking that indicates the level of protection required for the information to be removed or reduced. This can refer to both electronic media and hard copy information. Information that is not destroyed needs the originator's approval to be released at a lower level.

Term	Definition
SCI	Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Intelligence Community. See also Compartmented marking, Need-to-know.
Security	The controls and measures that an organisation uses to protect their people, information and assets.
Security breach	An accidental or unintentional action that leads or could lead to the loss or damage of official information or resources. A breach is also a failure to observe the protective security mandatory requirements. See also Security infringement and Security violation.
Security container or room	A container used to secure protectively-marked information or assets. This includes NZSIS-approved A, B or C class container or room. See Security Zones and Risk Mitigation Control Measures.
Security culture	A set of security related norms, values, attitudes, and assumptions that are inherent in the daily operation of an organization which is reflected in the actions and behaviors of personnel within the organisation.
Security incident	A security incident is an event caused by an individual or group that has or could have resulted in loss or harm to an organisation's assets, information or people, or an action that breaches the organisation's security procedures
Security infringement	Any incident that violates internal protective security procedures as outlined in internal agency protective security procedures, other than those that can be categorised as a security breach or security violation.
Security investigation	An investigation carried out to establish the cause and extent of a security incident that has, or could have, compromised the New Zealand government. The overall purpose of a security investigation is to prevent the incident from happening again by making improvements to the agency's systems or procedures.
Security policy	A set of rules, expectations, and overall approach that an organisation uses to protect people, information, and assets from security risks.
Security plan (ICT system)	A security plan is a formal document that provides detailed management, operational and technical information about an ICT system, its security risks and requirements and describes the controls in place or planned to meet those requirements. See also Security risk management plan.
Security procedure	Detailed step by step set of necessary activities that perform a specific security task or function.
Security risk	Any event that could result in the compromise, loss of integrity or unavailability of official information or resources, or the deliberate harm to people measured in terms of its probability and consequences.
Security violation	A deliberate, negligent or reckless action that leads, or could lead, to loss, damage, corruption or disclosure of official information or resources.

Term	Definition
Security zones	A method of assessing the security of areas used for protecting people, or handling and storing information and physical assets, based on security controls. Security zones range from One to Five.
Security-in-depth (or defence-in-depth)	A multi-layered, systematic approach to security in which security countermeasures are combined to support and complement each other. This makes unauthorised access difficult, for example, physical barriers should complement and support procedural security measures and vice versa.
Security risk management plan (SRMP)	Risk management: Security risk management plan. A plan that sets out how an organisation will manage their protective security risks. ICT Systems / NZISM: SRMPs identify security risks and appropriate treatment measures for ICT systems.
Site	A site is a spatial location that situates something, typically a physical structure, facility, or building but can also include a historical monument location, aircraft, or ship. See also: Facility.
Site Security Plan (SSP)	A site security plan documents measures required to counter identified risks to an organisation's function at resources at a site; and articulates how the site-specific security elements work together to form the required security in depth. It also explains the reasoning for the security controls chosen.
Stewardship	Stewardship is the careful and responsible management of something. In the context of this guide, it is the careful and responsible management of government information to benefit all New Zealanders.
Threat	A source of harm that is deliberate or has the potential or intent to do harm.
Threat assessment	Evaluation and assessment of the intentions of people who could pose a hazard to a resource or function, how they might cause harm and their ability to carry out their intentions. Threats need to be assessed to determine what potential exists for them to actually cause harm.
Treaty	A treaty is an agreement between states (countries) that is binding by international law. In some cases, international organisations can be parties to treaties. A treaty may also be called a convention, protocol, covenant or exchange of letters.

Term	Definition
Unauthorised access	To facilities or assets: Access to official facilities or assets that is not sanctioned by government policy or agency direction or an entitlement under legislation. To information: Access to official information that is not based on a legitimate need to know, sanctioned by government policy or agency direction or an entitlement under legislation.
Unauthorised disclosure	The communication or publication of official information where it is not based on a legitimate need to know, sanctioned by government policy or agency direction or an entitlement under legislation.
Unclassified information	Unclassified information is government information that would have a low impact on individuals, organisations or New Zealand's national interest if it were compromised. It doesn't need special security or handling over and above the standard protections that apply to all government information and therefore does not require classification or protective marking to keep it secure.
Visitor	A visitor is any person whose duties do not normally require them to access the area being visited, or who does not qualify for an appropriate pass, but who can demonstrate a legitimate reason for seeking entry to the area.
Vulnerability	ICT systems: A flaw, bug or misconfiguration that can be exploited to gain unauthorised access to a network or information. Risk management: The degree of susceptibility and resilience of an agency to hazards.
Wireless communication	Transmission of data over a communications path using electromagnetic waves rather than a wired medium.