Security Plan

Date authorised: 17 September 2025

Context

This is the guiding document relating to protective security in the PC. It reflects requirements set out in the Australian Government's Protective Security Policy Framework (PSPF) and articulates how the PC engages with, and uses, proportionate security measures and manages protective security risks to protect our people, information and/or assets.

It takes account of the nature of the PC's work and operations. It aims to achieve a balance between the effective management of security risks and the operational needs and realities of the Commission.

Objectives

The Commission aims to ensure:

- protective security risks are identified and mitigated.
- measures taken to mitigate risk are proportionate and protect the PC's people, information and assets.
- protective security measures are designed and implemented in accordance with PSPF requirements.
- All PC staff are aware of, and fulfil their roles and responsibilities in developing, implementing, and managing the security measures designed to protect people, information, and assets.

Scope

This plan, and related plans, policies and procedures, applies to:

- the Chair
- Commissioners
- staff employed under the Public Service Act 1999 (PS Act)
- contractors
- external third parties including individuals (e.g., visitors to Commission offices), and external service providers (including any subcontractors).

Legislative and policy context

The PSPF applies to all APS agencies subject to Public Governance, Performance and Accountability Act 2013 (PGPA Act).

The Department of Home Affairs is responsible for protective security policy, and administration of the PSPF. It is reviewed annually to ensure it reflects the current threat environment. Updates culminate in an annual release.

The PSPF comprises five tiers:

- **Principles** – apply to all aspects of protective security.
- **Protective security domains** – six interconnected subject areas.
- **Policy**[1] – includes detail of requirements[2] that entities must apply.
- **Standards and Technical Manuals** – detail additional mandatory requirements for specific areas of the PSPF. These include manuals maintained by Technical Authority Entities.
- **Guidelines**[3] – provide advice and examples to assist entities in implementing the requirements and standards.

[1] PSPF Annual Release 2025 | Protective Security Policy Framework
[2] PSPF Release 2025 – List of Requirements | Protective Security Policy Framework
[3] PSPF Guidelines 2025 | Protective Security Policy Framework

Security Principles

The Commission is committed to upholding and promoting the PSPF security principles:

1	Security is everyone's responsibility.
2	A positive embedded security culture is critical.
3	Security enables the effective and efficient delivery of Government business.
4	Security standards are implemented within the PC's unique risk environment to protect people, information, and assets.
5	The Chair, as the accountable authority, is responsible for security risks within the PC and the PC's impact on shared risks.
6	An action, evaluation and learning cycle is applied in response to security.

The PC's protective security framework

This plan and supporting plans and procedures set out the measures designed to protect the PC's people, information and assets.

PSPF Domains	PC Framework
Governance	▪ Security Plan ▪ Procurement Procedures - Contracted Providers
Risk	▪ Security Plan ▪ Enterprise Risk Management Framework ▪ Business Continuity Plan
Information	▪ Information Assets Framework ▪ PC Records Authority ▪ Information Assets Management Policy ▪ NAP policy
Technology	▪ DT Security Policy ▪ Acceptable Use of DT Policy ▪ Systems Asset Register ▪ Cyber Incident Response Plan ▪ Fortress Procedures
Personnel	▪ Security Clearance Procedures ▪ Staff Separation Procedures ▪ Pre-Employment Screening Procedures
Physical	▪ Physical Security Plan ▪ Duress Alarm Procedures ▪ Access Pass Procedures

Roles and responsibilities

The Chair, as agency head, is the accountable authority for the purposes of the PSPF and ultimately accountable for security in the PC.

Security arrangements support an entity's business objectives by identifying and managing security risks that could adversely affect achieving those objectives.

The Chair and Chief Security Officer (CSO) determine the security arrangements required for:

- the safety of personnel (including contractors) and those who have dealings with the PC. (including visitors).
- protection of resources, information and assets held by the PC.
- capacity to function, including during security incidents, disruptions, or emergencies
- vigilance, resilience, and adaptability of personnel to security risks.

Managers also have a responsibility to promote security awareness and ensure compliance with all protective security practices and procedures in place.

All employees have a responsibility to contribute to a positive security culture and meet their security obligations.

Governance

The following sets out the management structure and responsibilities relating to protective security.

Chief Security Officer (CSO) - Assistant Commissioner, Corporate Group

Appointed by the Chair, the CSO is responsible for directing all areas of protective security. The CSO is empowered to make decisions about the appointment of security advisors, security planning, risk management, and the investigation and response to security incidents. The CSO provides reports to Management Committee on security matters and seeks assistance from external sources as required.

Chief Information Security Officer (CISO) - Director, Digital Technologies

Responsible for the overall integrity and security of the PC's information security program This includes providing advice to the CSO on information security matters and risks relevant to the Commission's DT systems and information holdings.

DT Security Advisers - DT Operations Manager and Cyber Security Manager

Assist with the overall integrity and security of the Commission's DT systems. This includes providing advice to the CSO or CISO on DT security matters.

Agency Security Advisers (ASA) – Canberra and Melbourne

Responsible for the overall coordination of security activities and arrangements in the PC, with a particular focus on security of the PC's information holdings, personnel, and assets.

Managers

Responsible for promoting and ensuring compliance with protective security measures in the Commission. Also responsible for handling any local ad hoc security incidents/issues which require an immediate response and ensuring the CSO and/or ASA are informed of such incidents/issues in a timely manner.

Security Committee

Chaired by the CSO, the Committee's role includes reviewing and discussing risk exposure and security risk management measures and requirements.

Security awareness and training

The PC requires all employees to be security conscious - to be aware of, understand, and adhere to, protective security measures in place.

To support such awareness the PC will:

- promote security awareness as part of the induction of new employees
- provide regular training for all staff and managers in relation to physical, personnel and information security (including DT)
- publish guidance and resource material on SharePoint
- provide contact details of staff able to provide advice on security related matters.

Mandatory PSPF Directions

The PSPF provides that, having considered advice from key technical authority entities, the Secretary of the Department of Home Affairs may issue a direction to agencies to manage certain identified protective security risks posed to government. The Accountable Authority of each agency must adhere to any direction issued.

The PC will maintain a central register of all directions issued. The register will document how the PC has complied with each direction, including any addional mitigations or controls mandated.

Review

This security plan will be considered annually to decide if any updates are required.
It will be formally reviewed at least every two years. This review will include how the PC will:

- determine the adequacy of existing measures and mitigation controls
- respond to and manage any significant shifts in the PC's risk, threat and/or operating environment.

The principal resources used to review threats and implement security measures are:

- security risk reviews to identify security risks and threats to the PC's people, information, and assets
- appropriate security experts to be consulted for threat and criminal assessments
- the CSO via Management Committee
- the PC's Security Committee.

Risk

The concept of risk has two elements:

- the likelihood of something happening
- the consequences if it were to happen.

The level of risk is the product of these two elements.

Action taken to manage risk needs to address the likelihood of an event occurring, the consequences if it does occur, or both. While it is not possible nor desirable to have a totally risk-free environment, it is possible to manage risk by avoiding, reducing, transferring, or accepting risks and their likely consequences.

Security risks

A security risk is something that could cause harm to people or exposes PC information or assets to compromise, loss, unavailability, or damage.

Risk assessment

The PSPF requires the Chair, as the accountable authority, to determine the Commission's tolerance for security risks, supported by a transparent and justifiable process.

Risk tolerance is an informed decision to accept a risk. It is a practical application of risk appetite, which is the amount of risk an entity is willing to accept or retain within its tolerance levels and the limits of PSPF requirements.

Risk tolerance includes:

- expectations for mitigating, accepting, and pursuing specific types of risk
- boundaries and thresholds of acceptable risk taking
- actions to be taken or consequences for acting beyond approved tolerances.

Enterprise risk security management

Security risks relating to the PSPF requirements to safeguard PC data from cyber threats and ensure robust ICT systems are addressed in the PC's Enterprise Risk Management Framework:

Risk 4: '*Failure of critical business systems including cybersecurity breaches, data loss, compliance violations, ICT system failures, third-party risks, and insider threats*.

Security risks relating to the PC's capacity to function, including during security incidents, disruptions, or emergencies, are also addressed in the PC's Business Continuity Plan.

To strengthen our protective security posture and align with PSPF guidance, the PC will integrate the management of all PSPF domain risks into the PC's Enterprise Risk Framework.

Review

Date	Version	Changes made	Author(s)
September 2025	1.0	Review and combination of 2023 Security Policy and Security Risk Management Plan to align with changes to PSPF structure and approach.	[redacted]

Approval

Consultation	Approved by	Name	Date
Management Committee	Head of Office	[redacted]	17 September 2025