Australian Government
Department of the Prime Minister and Cabinet

Department of the Prime Minister and Cabinet Security Framework

Security Team

Introduction

The Department of the Prime Minister and Cabinet (PM&C) Security Framework (the Framework) outlines the Department's security policies and guidelines. Combined, these documents provide detailed guidance on protective security in PM&C. This Framework is designed to support the Department with the implementation of security measures commensurate with its security environment and meet the requirements outlined in the Australian Government Protective Security Policy Framework (PSPF). In addition, the Framework supports the continual growth of the Department's security maturity and provides guidance on how to undertake business operations in a manner that also safeguards our people, information and assets.

While best efforts have been made to provide clear security guidance across PM&C's operating environment, there may be circumstances where additional support is required to appropriately manage Departmental security risk. For support with interpreting requirements set out in this framework or to work through security complexities not appropriately covered in the below policies and guidelines, please contact PM&C Security Team at s 47E(d) @pmc.gov.au or by calling s 47E(d) (24 hours).

Security Assurance Policy

Security assurance is aimed at ensuring that PM&C's protective security risks are effectively managed, and that information is gathered and analysed to inform policy decisions meet our protective security obligations.

s 47E(d)

All PM&C staff must be aware of the guidelines in the Security Assurance Policy, and actively consider security in their day to day work, in their activities outside of work, and when they travel for personal or official reasons.

s 47E(d)

s 47E(d)

1. Security Awareness and Training Guideline

1.1. All PM&C staff must complete face-to-face induction training, or equivalent initial security awareness training, **within four weeks of joining the Department**. Staff must also complete an annual security refresher course every calendar year.

1.2. s 47E(d)

s 47E(d)

Induction training

1.5. All staff working in PM&C tenancies or with PM&C systems – including secondees, contractors and consultants – are to complete mandatory induction training within four weeks of commencement. s 47E(d)

1.6. Staff who do not complete their mandatory training may have their access to the Department's tenancies and ICT systems revoked.

1.7. Staff will receive notification from the PM&C Security Team regarding training attendance.

Refresher training

1.8. Staff are required to complete annual online security awareness training.

1.9. s 47E(d)

s 47E(d)

[redacted]

3. Security of PM&C Tenancies Guideline

3.1. The PM&C Security Team has access to all areas, including the equipment within, and may access these from time to time to ensure ongoing compliance with the PSPF and the Framework. s 47E(d)

[redacted]

4. s 47E(d)

[redacted]

s 47E(d)

[redacted]

Building construction, security zoning and physical security

4.10. The PM&C Security Team is to be consulted at the inception of projects involving the selection of new tenancies or the modification of existing tenancies. Consultation ensures security risks are considered and security is properly integrated into construction.

s 47E(d)

[redacted]

s 47E(d)

[redacted]

5. Security Reporting Guideline

5.1. Staff must report the compromise of official resources, for example their loss, misuse, unauthorised access, modification, disclosure or any interference. Staff should also report any suspicious incidents or suspicious contact from persons within or outside of PM&C. s 47E(d)

[redacted]

s 47E(d)

[redacted]

Information Security Policy and Guidelines

7. Information Security Policy

7.1. Information security is focused on protecting the Department's official information, preventing significant damage to the Department's reputation and/or compromise of national security.

- Staff must maintain a secure environment and protect official information by:
- Maintaining appropriate information security – through the proper use, storage, transfer, handling and disposal of material
- Applying the 'need-to-know' principle and the Clear desk policy
- Being aware of protective markers and how they are applied
- Mitigating information security risks
- Reporting information Security breaches to the PM&C Security Team.

7.2. All PM&C staff must be aware of the guidelines in this Information Security Policy, and actively consider the security of information in PM&C tenancies, but also when travelling for official purposes or working from the home.

s 47E(d)

s 47E(d)

s 47E(d)

The need-to-know principle

A person's rank or position of authority in the Department or any other organisation does not provide an automatic 'need-to-know'. Granting access to classified material because it is convenient to do so, is not a valid reason to provide access.

8.5. In line with the need-to-know principle, s 47E(d) information should only be made available to individuals who require access in order to do their work.

8.6. s 47E(d)

8.7. Security classified information is only to be accessed by staff who hold the minimum security clearance s 47E(d)

Further guidance and key contacts

To provide guidance in the application of legislative requirements the Australian Government has produced the following policy documents. These documents assist agencies in addressing their responsibilities for the protection of official resources (i.e., people, information and assets):

The Protective Security Policy Framework (PSPF) – developed by the Department of Home Affairs; and

The Australian Government Information and Communications Technology Security Manual (ISM) – developed by the Australian Signals Directorate.

s 47E(d)