



# **Government of South Australia**

**Department of the Premier and Cabinet Circular**

**PC030 – Protective Security Management Framework**

**February 2012**

# PROTECTIVE SECURITY MANAGEMENT FRAMEWORK

## TABLE OF CONTENTS

<b>TABLE OF CONTENTS</b>	<b>2</b>
<b>1. PURPOSE</b>	<b>3</b>
<b>2. SCOPE</b>	<b>3</b>
<b>3. BACKGROUND</b>	<b>3</b>
<b>4. ROLES AND RESPONSIBILITIES</b>	<b>4</b>
<b>5. PROTECTIVE SECURITY POLICY FRAMEWORK</b>	<b>5</b>
5.1 <i>Security Risk Management</i>	5
5.2 <i>Information Security</i>	6
5.3 <i>Personnel Security</i>	7
5.4 <i>Physical Security</i>	7
5.5 <i>Procurement Security</i>	8
5.6 <i>Security Incidents and Investigations</i>	8
5.7 <i>Security when Working Away from the Office</i>	9
5.8 <i>Exceptional Circumstances - Waiver of certain provisions</i>	10

# 1. Purpose

- 1.1. The Protective Security Policy Framework supports the South Australian Government's risk management policy through the requirement for a risk-based approach for the protection of assets and resources, to minimise disruption to service delivery and Government operations.
- 1.2. This circular outlines the strategic approach approved by Cabinet for a whole of government protective security policy, based on the principles outlined within the Australian Government's Protective Security Policy Framework.
- 1.3. The Framework addresses the security requirements for Government assets through the application of minimum standards in each of the areas comprising the protective security regime, in order to appropriately treat identified risks.

# 2. Scope

- 2.1 The Protective Security Policy Framework applies to all South Australian Government public authorities, including but not limited to, public sector agencies (as defined in the *Public Sector Act 2009*), administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown. Public authorities are hereinafter referred to as "Agencies".
- 2.2 The Protective Security Policy Framework is outlined on the website of the Commonwealth Attorney-General's Department, at <http://www.ag.gov.au/Protectivesecuritypolicyframework/Pages/default.aspx>

# 3. Background

- 3.1. The South Australian Government is firmly committed to maintaining essential services and protecting the community as far as possible from harm. Objectives 17, 21 and 32 of the Government's State Strategic Plan, which convey the importance of improving public sector performance and the State's wellbeing through safe and secure communities, express this commitment. In the broader Australian context South Australia has obligations to work with other jurisdictions in sharing information to provide this protection to our respective communities. These commitments impose strict requirements on the Government and its Agencies.
- 3.2. Agencies need to provide proper security for their functions and official resources to ensure they do not place themselves or the Government at risk and potentially undermine public confidence in South Australia's democratic institutions. Community perceptions of government rest in part on its trust that government will be able to function in any circumstances and fulfil its proper role.

- 3.3. The Protective Security Policy Framework is designed to assist in the adoption of a culture which recognises the importance of protecting the assets which the Public Sector relies on to fulfil its responsibilities and provide services the community.
- 3.4. When security considerations are included in the corporate planning process, the security plan will assist with meeting business needs, providing a safe working environment for staff and adding value to an agency's relationship with its clients.
- 3.5. Security planning and risk treatments need to be focussed on areas of significant risk. Security planning should therefore involve an analysis of the risks to determine whether they are significant and warrant treatment. Security plans should provide treatments that are appropriate to the level of risk and be cost-effective.

## 4. Roles and Responsibilities

- 4.1 The Government is responsible for the security of all State assets. Individual Ministers are responsible for the security of assets in their portfolios.
- 4.2 The Protective Security Policy Framework identifies the policies and guidelines to be followed for achieving consistent security standards within and across the South Australian Government. The Protective Security Policy Framework recognises that security risk management is the responsibility of all public sector employees and places accountability on Chief Executives to ensure that strategies are developed and implemented consistently within the Government's overall risk management policy and framework.
- 4.3 A Chief Executive must:
  - 4.3.1 Develop, implement and maintain an Agency Security Plan in accordance with the minimum standards described in the Australian Government Protective Security Policy Framework . This Plan must be specifically designed for the Agency's functions and the security risks faced in its business operations.
  - 4.3.2 Ensure responsibility for protective security matters, including the development of policies and procedures, a security management compliance program and that its performance outcomes/operations are assigned to a designated Agency Security Executive.
  - 4.3.3 Appoint an Agency Security Adviser who regularly reports to the Agency Security Executive. The Agency Security Adviser is responsible for the protective security function on a day-to-day basis and should provide relevant briefings to the Agency Security Executive as required, as well as be available to provide appropriate advice to Agency employees about security risk management issues.
  - 4.3.4 Appoint an IT Security Adviser, who regularly reports to the Agency Security Executive. The IT Security Adviser is responsible for the protection of the security of information and communication technology on a day-to-day basis; providing relevant briefings to the Agency Security Executive as required; and

should be available to provide appropriate advice to Agency employees about security risk management issues. CTO Notification 89 (issued by the Office of the Chief Information Officer) provides information about this role, including guidance on the selection of suitable persons to fill the role. It also details the relevant qualifications and accreditations that an IT Security Adviser should hold and maintain.

4.3.5 Develop, implement and maintain a protective security compliance program with documented policies, systems, procedures, internal controls and management reporting to ensure that security risks are appropriately managed and that the Protective Security Policy Framework is robustly applied.

4.4 The Auditor-General performs professional independent audits of agencies, and reports to Parliament. The *Public Finance and Audit Act 1987* provides a mandate for the Auditor-General to conduct different types of audit.

The types of audit include financial and compliance audits and reviews of the adequacy of controls at agencies. These audits and reviews consider the integrity of an agency's accountability responsibilities, the nature of compliance with legal, policy and procedural obligations, and the adequacy of controls to safeguard resources and assets made available to agencies.

Through these audit processes the Auditor-General may review an agency's protective security compliance program and assess it in the context of the Protective Security Policy Framework.

## 5. Protective Security Policy Framework

### 5.1 Security Risk Management

5.1.1 The Chief Executive of an agency is accountable for the development and management of an Agency Security Plan.

5.1.2 The Agency Security Plan must be developed to manage the agency's security risks and should be based on a security policy that supports the Agency's goals and resources.

5.1.3 Security risks are to be managed in accordance with ISO 31000:2009 and the principles of the South Australian Government Risk Management Policy Statement.

5.1.4 The Agency Security Policy must address the following key areas:

- Information Security
- Personnel Security
- Physical Security
- Procurement Security
- Security Incidents and Investigation
- Security When Working Away from the Office

- 5.1.5 The Agency Security Plan and associated policies and procedures must be developed in accordance with the minimum standards described in the Australian Government Protective Security Policy Framework.
- 5.1.6 An agency's risk management treatments must be appropriate to the level and type of risk and the importance of the function or resource.

### **Resources**

South Australia Police - Police Security Services Branch provides security risk management advice on a fee-for-service basis. This advice extends to agency security plans along with staff awareness training. Suitably qualified private sector service providers, as well as ASIO's T4, can provide similar support on a fee-for-service basis.

## **5.2 Information Security**

- 5.2.1 The Chief Executive of an Agency is accountable for protecting information resources in accordance with the minimum standards described in the Australian Government Protective Security Policy Framework.
- 5.2.2 Information resources include documents, papers, data and intellectual knowledge along with information and communication technology (including computing and communications systems).
- 5.2.3 In relation to the security of information and communication (including cyber) technology, Agencies (and Agency suppliers with relevant contractual requirements) are required to comply with the *South Australian Government Information Security Management Framework*.
- 5.2.4 If a compromise of official information could cause harm to the Government, agencies, the public interest or other entities or individuals, Agencies must consider giving the information a security classification.
- 5.2.5 All Agencies must apply and use the security classification system described in the Australian Government Protective Security Policy Framework.
- 5.2.6 Official information can only be disclosed subject to the authorisation of an agency's Chief Executive. The authorisation must be clearly stated, not implied, and is subject to the provisions of the *Freedom of Information Act (SA) 1991* (the FOI Act). In relation to personal information, the authorisation must comply with the Information Privacy Principles contained in Premier and Cabinet Circular No 12, which incorporates Cabinet Administrative Instruction No 1 of 1989 (Information Privacy Principles Instruction).
- 5.2.7 A public sector employee must comply with the provisions of the Public Sector Code of Ethics in relation to handling official information.

### **Resources**

The Office of the Chief Information Officer (OCIO) provides advice to South Australian Government Agency personnel on cyber security matters.

### **5.3 Personnel Security**

- 5.3.1 The Chief Executive of an agency is responsible for assuring the integrity of personnel employed by the agency.
- 5.3.2 The security of any agency relies on the integrity of its employees and contractors. All government employees must meet the standards of probity as defined in the Code of Ethics'. An agency's recruitment process, probationary programs, performance management policies and general operations must be designed to ensure the integrity and honesty of all its employees.
- 5.3.3 The Commissioner for Public Employment is responsible for promoting public service principles in accordance the *Public Sector Act 2009* (and in particular, Sections 14, 15, 16 and 22 of this Act), and the Public Sector Regulations 2010
- 5.3.4 Access to official and security classified information must be restricted on a 'need to know' basis. In addition, all persons accessing security classified information must be 'cleared' in accordance with the system and minimum standards described in the Australian Government Protective Security Policy Framework.

#### **Resources**

Department of Premier and Cabinet

Cabinet and Policy Coordination facilitates personnel vetting services for all South Australian Government agencies.

### **5.4 Physical Security**

- 5.4.1 The Chief Executive Officer of an agency is accountable for implementing physical security measures designed to safeguard the people, assets and information associated with the Agency.
- 5.4.2 Physical security measures comprise the risk treatments implemented following a *Security Risk Review* and can be achieved through a combination of policies, procedures and physical attributes that will protect people, assets and information.
- 5.4.3 Physical security measures contribute towards the employer's obligations described by the *Occupational Health Safety and Welfare (SA) Act 1986*.
- 5.4.4 Physical security measures must be implemented in accordance with the mandated requirements described in the Australian Government Protective Security Policy Framework.
- 5.4.5 On 17 July 2006 Cabinet approved the introduction of a Government *Protective Security Policy*, The policy mandates South Australia Police (through Police Security Services Branch) as the supplier of protective security services to designated government critical infrastructure and high risk assets, and a whole of government

alarm monitoring service. Agencies must comply with the requirements of the Government Protective Security Policy.

### **Resources**

South Australia Police - Police Security Services Branch provides a range of security services to government Agencies on a fee-for-service basis. These services include security guards, patrols and monitoring of CCTV. Other private sector providers provide similar services on a fee-for-service basis for physical security requirements that are not mandated to be provided by South Australia Police.

Police Security Services Branch is the mandated provider of security alarm monitoring services to all South Australian Government Agencies and protective security services to designated government Critical Infrastructure-High Risk assets.

## **5.5 Procurement Security**

- 5.5.1 The Chief Executive Officer of an agency is responsible for ensuring the integrity of procurement processes undertaken by that Agency.

The State Procurement Board issues and reviews policies, principles and guidelines relating to the procurement operations of public authorities, in accordance with Section 12 of the *State Procurement Act 2004*.

- 5.5.2 Procurement processes must incorporate security requirements in accordance with the minimum standards of the Australian Government Protective Security Policy Framework.

### **Resources**

Department of Treasury and Finance

The State Procurement Board is responsible for setting the policy, standards, guidelines and conduct for the procurement of goods and services across the public sector.

## **5.6 Security Incidents and Investigations**

- 5.6.1 The Chief Executive Officer of an Agency is responsible for ensuring that security incidents are reported and investigated.

- 5.6.2 Agencies must have guidelines for reporting, recording and investigating security incidents. A record of incidents will help an Agency identify and treat risks. Additional guidelines should outline procedures to conduct security investigations, adopting a consistent approach that ensures the Government is not further compromised during an investigation.

- 5.6.3 South Australia Police are responsible for receiving and investigating reports of crime. Agencies need to develop policies and procedures for reporting and investigating

incidents that impact on the security of persons, assets and information. Many incidents occur that do not constitute a criminal offence but do impact on security risks.

- 5.6.4 Security incident reporting and investigation policies must be developed in accordance with the minimum standards described in the Australian Government Protective Security Policy Framework.
- 5.6.5 Agencies must report cyber security incidents to the Office of the Chief Information Officer in accordance with Information Security Management Framework (ISMF) Standard 140: Notifiable Incidents.

### **Resources**

South Australia Police

In an emergency contact police by ringing 'triple zero (000)'.

Reports for non-urgent police assistance should be directed to telephone 131 444 or the nearest police station.

State Protective Security Branch provides advice in relation to reporting and investigation of security incidents.

Department of the Premier and Cabinet

The Office of the Chief Information Officer (OCIO) provides advice in relation to the reporting and management of ICT-based security incidents.

## **5.7 Security when Working Away from the Office**

- 5.7.1 The Chief Executive Officer of an agency is responsible for the implementation of policies and procedures to ensure the security of persons, assets and information associated with work undertaken by Agency employees away from their office workplace.
- 5.7.2 The Commissioner for Public Employment has issued Commissioner's Standards which include general provisions that relate to working at home.
- 5.7.3 Security policies for work conducted away from the office must be developed in accordance with the minimum standards described in the Australian Government Protective Security Policy Framework.

### **Resources**

South Australia Police - Police Security Services Branch provides security risk assessment advice for home-based work, on a fee-for-service basis. Private sector service providers can provide similar advice on a fee-for-service basis also.

Commissioner for Public Employment – Commissioner's Standards

<http://www.espi.sa.gov.au/page-61>

## **5.8 Exceptional Circumstances - Waiver of certain provisions**

5.8.1 If an Agency is unable to comply with a mandatory requirement described in the Australian Government Protective Security Policy Framework, (other than the pre-excluded requirements identified in 5.8.2 below), or a mandatory policy/standard described in the South Australian Government Information Security Management Framework, the agency Chief Executive may only waive that requirement in limited circumstances, and only for:

- A defined purpose, and
- A nominated period.

It should be noted that some mandatory requirements relating to personnel security and information security can not be waived.

5.8.2 Mandatory requirements GOV-7 and GOV-13 from the Australian Government Protective Security Policy Framework do not require an agency Chief Executive to issue a waiver or exemption as they do not apply to the South Australian Government.

5.8.3 If a proposed waiver could impact on the protection of the information of another Government agency or from another jurisdiction, that agency, the Office of the Chief Information Officer and the other jurisdiction (where another jurisdiction is involved) must be consulted before the waiver is granted.

5.8.4 Agencies must maintain a record of any waiver issued. The record should include the submission to the agency's Chief Executive identifying associated security risks and the measures implemented to mitigate that risk.

5.8.5 If an agency Chief Executive decides to waive a mandatory requirement, advice of that decision along with its purpose and the time frame must be provided to:

- The Chief Executive, Department of Premier and Cabinet, and
- The Commissioner of South Australia Police.
- In the case of cyber (ICT) standards, the Chief Information Officer must also be advised of that decision (in addition to the above positions), including the purpose of the waiver and the time frame.