VICTORIAN GOVERNMENT CIO COUNCIL

Information Security

Information Security Management

Policy

Specified Victorian Government departments, agencies and State-owned enterprises (collectively referred to as 'agencies' hereafter) must implement a revised set of approved Victorian Government policies, standards and guidelines for information security.

Keywords:	Security policy, framework, ISM, PSPF.	
Identifier: SEC POL 01	**Version no.:** 2.0	**Status:** Final
Issue date: 1 October 2012	**Date of effect:** 1 October 2012	**Next review date:** 1 November 2014
Authority: Victorian Government CIO Council	**Issuer:** Victorian Government Chief Technology Advocate	

Overview

Policy objectives

The objectives of this Victorian Government (VG) information security policy are to deliver:

- greater efficiency and value for money in the investment of departments and agencies in information security, by adoption of a common approach;
- improved levels of co-ordination and confidence between agencies in sharing data;
- a common basis for cross-agency initiatives; and
- consistent protection of the State's systems and data.

Policy statement

Specified Victorian Government departments, agencies and State-owned enterprises (collectively referred to as 'agencies' hereafter) must implement a revised set of approved Victorian Government policies, standards and guidelines for information security. In particular, they must implement the *SEC STD 01 Information Security Management Framework and SEC STD 02 Critical Information Infrastructure Risk Management.*

Frameworks under which the policy will operate

The revised set of policies, standards and guidelines will be based primarily on two Australian Government frameworks, which have been adapted to Victorian Government requirements:

- the *Protective Security Policy Framework* (PSPF), managed by the Attorney-General's Department (AGD), insofar as it applies to Information and Communications Technology (ICT) information, people, processes and assets; and
- the *Information Security Manual* (ISM), managed by the Defence Signals Directorate (DSD).

These frameworks are based on industry standards such as ISO 27000.

- Other Australian Government Frameworks may also be adopted where appropriate. For example, the National eAuthentication Framework (NeAF) has already been adapted for use in Victorian Government identity and access management standards and is directed for use in the PSPF Information Security mandatory requirements.

Rationale

Information and Communications Technology (ICT) has fundamentally changed the way in which the Victorian Government conducts business. The Government is now **dependent** on information and communications to deliver services to the Victorian public, and to efficiently manage internal Government operations.

However, information and communication technology has significant risks, including unprecedented and escalating levels of external threats to information security and privacy.

The Government-wide adoption of common policy, standards and processes for information security (including related personnel security and physical security) allows the Victorian Government to reduce these risks.

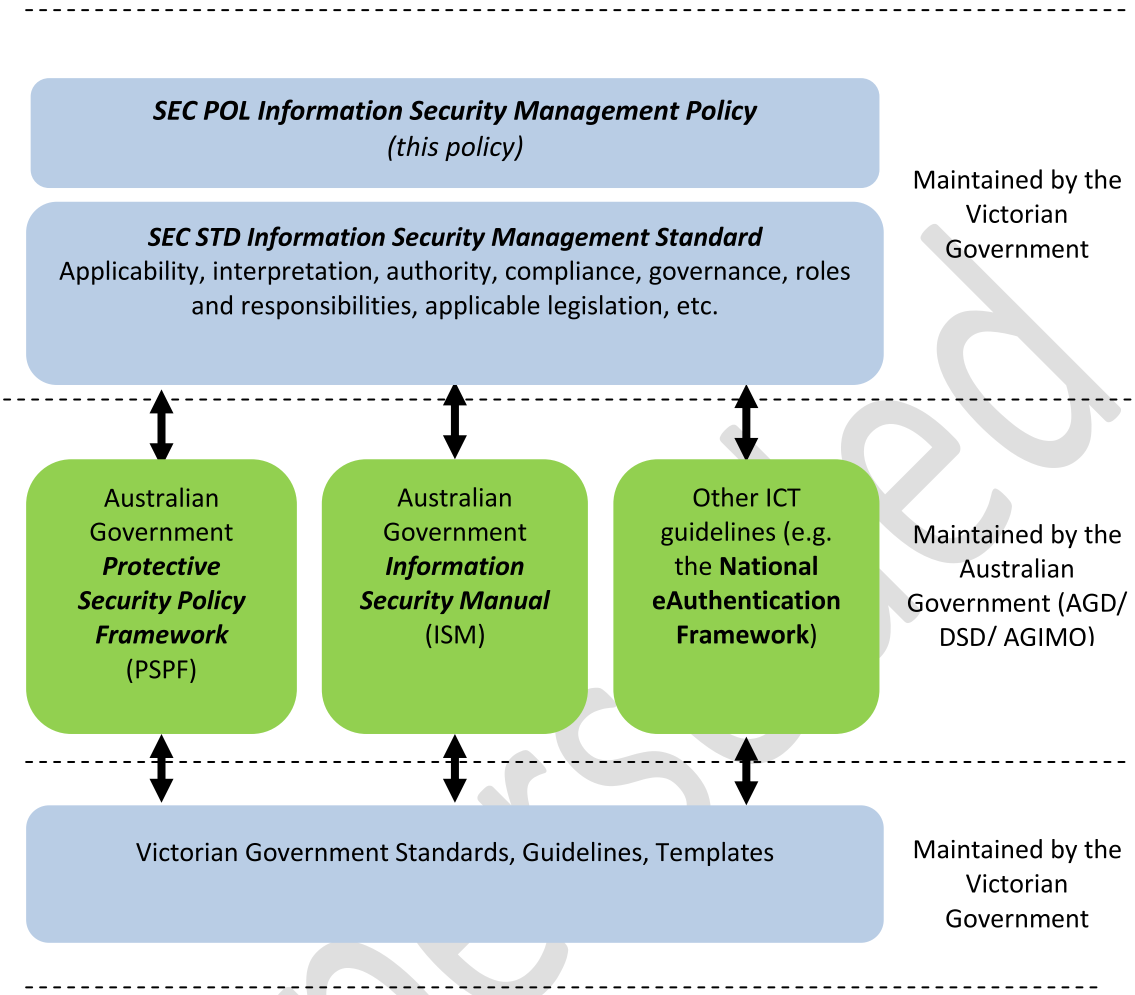
The rationale for a Victorian Government framework for information security is based on the following findings:

1. Some agencies have to consider aspects of information security policy which are unique, or may face agency-specific risks, or may have to implement particular security controls, but there is a common core of policy, risks, and controls that apply to all agencies; and
2. Information is increasingly being shared within and across agencies, requiring a common approach to information security.

The rationale for adopting Australian Government frameworks is:

- The AGD PSPF and the DSD's ISM are consistent with the risk-based approach mandated by the Victorian Government Risk Management Framework;
- Adopting a national framework enables more efficient information sharing across multiple jurisdictions;
- The PSPF and ISM are based on the AS/NZS ISO 27000 and are consistent with previous and current Victorian Government information security policy;
- The Australian Government threat environment is equally applicable to State Government;
- The ISM provides agencies with a set of detailed controls that can be implemented to mitigate risks to their information and systems. Agencies are required to make informed, risk-based decisions specific to their unique environments, circumstances and risk appetite; and
- The ISM provides a more substantive set of controls than ISO27002 with qualitative and evidence-based control recommendations (see Figure 1).

Figure 1: Structure of the Revised Victorian Government Information Security Management


SEC POL Information Security Management Policy
(this policy)
SEC STD Information Security Management Standard
Applicability, interpretation, authority, compliance, governance, roles and responsibilities, applicable legislation, etc.
Maintained by the Victorian Government
Australian Government ***Protective Security Policy Framework*** (PSPF)
Australian Government ***Information Security Manual*** (ISM)
Other ICT guidelines (e.g. the **National eAuthentication Framework**)
Maintained by the Australian Government (AGD/ DSD/ AGIMO)
Victorian Government Standards, Guidelines, Templates
Maintained by the Victorian Government

While the 'core' of these information security frameworks will be maintained by others, there will still be an ongoing requirement for some Victorian Government information security

- policies (such as this policy);
- standards (e.g. as a result of Victorian Government ICT procurement processes resulting in the use of a specific technology, or Victorian Government agreements to use a specific authoritative source for guidance on specific ICT issues, etc.);
- guidelines (e.g. to enable re-use of collective ICT 'best practice' information derived from surveys of agencies, or to provide detailed information or clarifications to support the high level requirements in the PSPF or ISM); and
- templates (e.g. for Victorian Government reporting).

Scope

This policy applies to all Victorian Government departments and Victoria Police, VicRoads, State Revenue Office, Environment Protection Authority, Public Transport Victoria, Country Fire Authority, State Emergency Services, Ambulance Victoria, Emergency Services Telecommunications Authority, Metropolitan Fire and Emergency Services Board, and ICT shared services providers such as CenITex.

Where applicable, legal and or regulatory compliance obligations take precedence over this policy and related standards. Departments and agencies may have additional legal and or regulatory information protection compliance requirements. Examples include (but are not limited to) Victoria Police and the Commissioner for Law Enforcement Data Security (CLEDS), credit card processing contract obligations of the Payment Card Industry Data Security Standard (PCI DSS) and the Information Privacy Act 2000.

Compliance

Timing

The date given at the head of this policy is when the policy comes into effect, not the date for implementing the supporting standards or achieving compliance with standards.

Reporting

See Victorian Government SEC STD 01 and SEC STD 02 standards for details of compliance measurement and reporting.

Reference and Toolkits

Victorian Government standards: http://digital.vic.gov.au/policies-standards-guidelines/

Australian Government *Protective Security Policy Framework* (PSPF): http://www.ag.gov.au/Protectivesecuritypolicyframework/Pages/default.aspx

Australian Government *Information Security Manual* (ISM): http://www.dsd.gov.au/infosec/ism/index.htm

Australian Government *National eAuthentication Framework* (NeAF): http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html

Further information

For further information regarding this standard, please contact digital.government@dsdbi.vic.gov.au.

Glossary

Term	Meaning
AGD	Auditor General's Department
CIO	Chief Information Officer
DSD	Defence Signals Directorate
ICT	Information and Communications Technology
ISM	Australian Government *Information Security Manual*
NeAF	National eAuthentication Framework
PSPF	Australian Government *Protective Security Policy Framework*
VG	Victorian Government

Version history

Version	Date	TRIM ref	Details
1.0	September 2006	D09/122140	Final
1.1	December 2012	D12/238925	Review Draft 1 - Aligning to new template and policy and standards
1.2	February 2013		Review Draft 2
1.3	12 March 2013		ISAG Subgroup – review draft 3
1.4	20 March 2013		Draft 4 to wider ISAG for review