Guiding Principles

Victorian Protective Data Security Framework and Standards

Overview

Members of the Victorian community interact with government every day, and in almost every interaction, information is created, captured or collected. Given the vast volume of information processed or held by Victorian public sector (**VPS**) organisations secure management of public sector information, assets and services is critical to service delivery and public safety. By implementing protective security measures, VPS organisations can protect information against a range of threats.

The guiding principles of the Victorian Protective Data Security (**Framework**) and Victorian Protective Data Security Standards (**Standards**) enable VPS organisations to evaluate their current and prospective security practices.

Guiding Principles

1. **Strong governance** arrangements ensure the protective data security requirements of the business are reflected in organisational planning.

2. **Risk management** empowers an organisation to make informed decisions and prioritise security efforts.

3. Understanding **the value of information** informs an organisation's application of security measures to protect information.

4. A **positive security culture** with clear personal accountability and a mature understanding of managing risk, responsibility and reputation allows an organisation to function effectively and support the delivery of government services.

5. A **continuous improvement lifecycle model** enables an organisation to systematically identify opportunities to mature its protective data security practices.

6. Sound protective data security practices assist an organisation to achieve its objectives in an **efficient, effective and economic** manner.

February 2020 – Version 1.0

1. Governance

Principle 1: Strong governance arrangements ensure the protective data security requirements of the business are reflected in organisational planning.

The Australian National Audit Office (**ANAO**) defines 'public sector governance' as:

> *How an organisation is managed, its corporate and other structures, its culture, its policies and strategies and the way it deals with its various stakeholders. The concept encompasses the manner in which public sector organisations acquit their responsibilities of stewardship by being open, accountable and prudent in decision- making, in providing policy advice, and in managing and delivering programs*[1].

Given the breadth of organisations across the VPS, OVIC recognises that governance arrangements can take many forms. Under the Framework, your organisation is expected to establish security governance arrangements that reflect its individual circumstances, and base policies and processes on sound risk management. This approach balances the benefits and potential costs of protective data security activities, ensuring security measures reflect the value of information.

The evolving environment in which VPS organisations operate, and the need for enhanced secure information sharing practices across governments, highlight the critical function that public sector governance plays.

By initiating robust governance arrangements, your organisation can direct and control processes for the protection of your information. This includes senior management and executives prioritising protective data security through authority, accountability, stewardship, leadership, direction and ensuring all personnel understand their role in protecting information.

By embedding strong governance policies and practices and ensuring these measures reflect changing needs, your organisation will better prepared to face the challenges of protective data security.

2. Risk management

Principle 2: Risk management empowers organisations to make informed decisions and prioritise security efforts.

Within Victorian Government risk management is defined as

> *the combination of organisational systems, processes and culture which facilitate the identification, assessment, evaluation and treatment of risk to achieve an appropriate balance between realising opportunities while minimising losses in the pursuit of strategic objectives*[2].

A risk management approach requires your organisation to ensure information is always adequately protected, by continually assessing security measures against any new or updated threats and vulnerabilities.

[1] Australian National Audit Office Better Practice Guide, *Public Sector Governance*, Vol. 1 & 2, July 2003

[2] Department of Treasury and Finance, Victorian Government Risk Management Framework (VGRMF), March 2015

The adoption of a risk-based approach consistent with the Victorian Government Risk Management Framework (**VGRMF**) is the fundamental principle of the Framework and Standards. This flexible approach to implementing security measures provides your organisation with the autonomy to interpret your business needs and articulate your risk tolerance within your operating environment.

Senior management and executives are expected to understand, prioritise and manage security risks to prevent harm to information and disruption to business objectives.

3. Information value

Principle 3: Understanding the value of information informs an organisation's application of security measures to protect public sector data.

Value refers to the overall importance of information, based on a holistic assessment of potential compromise to the confidentiality, integrity and/or availability of information.

The overall value of information informs security measures needed to fully protect it. The Standards provide organisations with tools to assess this overall value.

Confidentiality, Integrity and Availability (**CIA**) are widely recognised as the traditional security attributes of information management and are commonly referred to as the CIA triad.

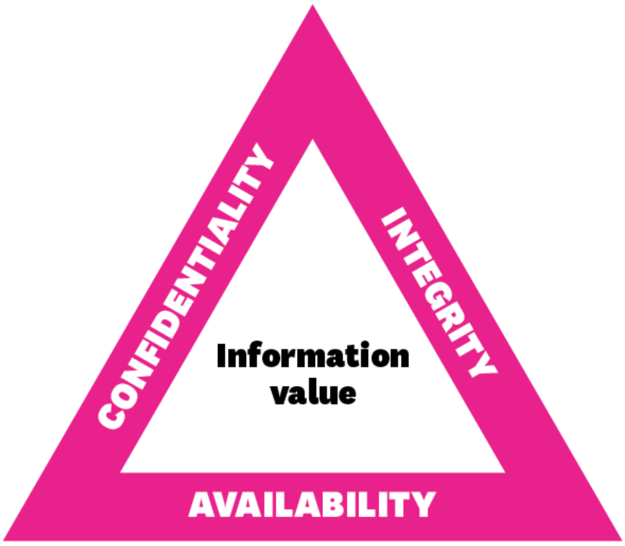

Figure 2. CIA Triad

Confidentiality	The limiting of official information to authorised persons for approved purposes (need to know).
Integrity	The assurance that information has been created, amended or deleted only by the intended, authorised means and is correct and valid.
Availability	The desired state that allows authorised persons to access particular information for authorised purposes, at the time they need to do so.

The Framework and Standards consider these three security attributes in an equal manner.

4. Security culture

Principle 4: A positive security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation allows an organisation to function effectively and support the delivery of government services.

Organisational culture is underpinned by the attitudes and behaviours of personnel and their shared values and beliefs that interact with the organisation's structures and control systems to produce behavioural norms[3]. Behavioural norms influence the day-to-day operation of an organisation and act as a powerful and often subliminal force that shapes its very nature.

The Framework and Standards seek to establish security as a natural element of organisational culture. To achieve this, organisations must introduce cultural change where protective data security practices are reflected in everyday business operations, and where all personnel take a shared responsibility. By embedding security in organisational culture, it becomes something that 'is', rather than something an organisation 'has' or 'does'.

A natural outcome of this cultural transformation program will:

- have personnel thinking and acting in more security-conscious ways;
- reduce organisations' protective data security risks; and
- enable the secure delivery of government services.

5. Continuous improvement (Plan, Do, Check, Act)

Principle 5: A continuous improvement lifecycle model enables an organisation to systematically identify opportunities to mature their protective data security practices.

A key concept used throughout the Framework and Standards is a continuous improvement lifecycle model. This is an underlying theme of international standards such as:

- AS/NZS ISO 31000 Risk management – Principles and guidelines;
- ISO 9001 Quality management; and
- ISO 19600:2014 Compliance management systems.

This quality-driven philosophy is designed to integrate protective data security into an organisation's entire business practices. It also ensures that security management including risk management, information management, personnel management, ICT management and physical management is not a 'set and forget' exercise.

The framework requires organisations to:

- **PLAN** – Contextualise their business objectives: understand the business and its core functions, and plan accordingly;

- **DO** – Integrate security measures proportionate to business risks: enhance business operations;

- **CHECK**– Consistently monitor business operations: undertake monitoring and assurance activities to ensure that implemented security measures support the business objectives while minimising business risks; and

[3] B. Uttal, 'The corporate culture vultures', *Fortune Magazine*, Vol. 108, No. 8, October 1983

- **ACT** – Review, validate and update business objectives, risks and operations based on lessons learned: ensure security measures are updated to support an agile business response to a dynamic environment.

By adopting this model, your organisation will systematically identify opportunities to mature your protective data security practices and secure information through all stages of its lifecycle.

6. Business objectives

Principle 6: Sound protective data security practices enable an organisation to achieve its business objectives in an efficient, effective and economic manner.

To deliver value to the Victorian Government and broader community, the VPS must transform the way it understands, uses and consumes information. This concept extends beyond the strict protective data security areas and reflects important principles and themes of information management principles.

A report published in December 2015 by the Victorian Auditor General: Access to Public Sector Information[4] stated that previous efforts to establish a "foundation of comprehensive and sound information management (**IM**) practices have been neglected", resulting in organisations not properly understanding nor managing the information they hold.

Organisations must have confidence in information they use when doing business, to enable maximum value (efficiency), ensure the delivery of quality outcomes (effectiveness) and minimise costs (economy).

By employing the protective data security measures of the Framework and Standards, your organisation can ensure the core attributes of your information (confidentiality, integrity and availability) are maintained, and have confidence that your information can be relied on to make quality decisions.S

The Framework and Standards enable your organisation to continually refine your security measures and respond to the changing needs of your internal business and the broader operational environment, including delivering value to the VPS.

Further Information

Contact Us

t: 1300 00 6842
e: enquiries@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer

This fact sheet does not constitute legal advice and should not be used as a substitute for applying the provisions of the Freedom of Information Act 1982 Privacy and Data Protection Act 2014, or any other legal requirement, to individual cases.

[4] Report available on the VAGO website - https://www.audit.vic.gov.au/report/access-public-sector-information?section=