Guidelines to protecting the security of personal information: ‘Reasonable steps’ under Information Privacy Principle 4.1

Issued January 2017
This page is intentionally left blank.
Guidelines to protecting the security of personal information: ‘Reasonable steps’ under Information Privacy Principle 4.1

Issued January 2017
# Guidelines to Protecting the Security of Personal Information Document Details

<table>
<thead>
<tr>
<th>DOCUMENT DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protective Marking</td>
</tr>
<tr>
<td>Publication Date</td>
</tr>
<tr>
<td>Document Status</td>
</tr>
<tr>
<td>Author</td>
</tr>
</tbody>
</table>
This page is intentionally left blank.
This page is intentionally left blank.
Introduction

Information Privacy Principle (IPP) 4.1 requires Victorian public sector organisations to take reasonable steps to protect the personal information they hold from misuse, loss, and unauthorised access, modification or disclosure.

Protecting the security of personal information is important. Robust security helps to minimise privacy breaches, maintain citizen trust in public organisations that collect and handle their personal information, and ensure that information assets – which are essential for decision-making – maximise public value creation.

IPP 4.1 does not prescribe what constitutes ‘reasonable steps’. The purpose of these guidelines is to assist Victorian public sector organisations to understand what this means and to help them meet this obligation.

The publication of these guidelines follows the release of both the Victorian Protective Data Security Framework (VPDSF or ‘the framework’) – which came into effect on 1 July 2016 – and the Victorian Protective Data Security Standards (VPDSS or ‘the standards’) – which were issued, and came into effect, on 28 July 2016. Consequently, these guidelines are designed to show the linkages between the ‘reasonable steps’ duty in IPP 4.1, and the VPDSF and VPDSS.

The framework and standards require organisations to adhere to a minimum set of protective data security requirements. They are based on national and international benchmarks. The framework and the standards cover all Victorian public sector information, not just the personal information covered by IPP 4.1. At the same time, they do not cover as broad a range of organisations as does IPP 4.1. For example, they do not expressly apply to local councils or universities.

The standards adopt a risk-based approach to protective data security. This approach is consistent with the IPP 4.1 requirement to take ‘reasonable steps’ to protect personal information. Both requirements recognise that security measures should be based on an organisation’s individual circumstances and the risks they need to manage. As circumstances and risks change over time, so too will the measures that are appropriate to identify and mitigate them. This office, therefore, regards the standards as being the ‘reasonable steps’ that the Victorian public sector must implement in order to meet IPP 4.1 obligations.

Given that the VPDSS sit within the broader protective data security framework developed by this office, the standards should not be read in isolation. For example, the overarching VPDSF principles (which inform the guiding principles in Part 3 of these guidelines) and the supporting security guides that are contained in the framework will inform the application of the standards. Organisations subject to the IPPs should therefore have regard to the framework in its entirety when ascertaining what steps are ‘reasonable’ to protect the personal information they hold.

1 ‘Personal information’ is defined in s. 3 of the Privacy and Data Protection Act 2014 as ‘information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies’. 
Context

IPP 4.1 imposes a statutory duty on the Victorian public sector. The duty is that Victorian public sector organisations that hold personal information must take ‘reasonable steps’ to protect it. This means that foreseeable security risks must be anticipated and necessary precautions taken to protect personal information and mitigate those risks.

If a Victorian public sector organisation – through action or inaction – fails to meet this requirement to take ‘reasonable steps’, it breaches that statutory duty. The relevant standard of care is set out in the VPDSF, which includes the VPDSS.

The steps outlined in this guide are not an exhaustive list of the security measures that can or should be taken. Organisations must be aware of any additional legal and regulatory requirements that bind them, including:

- Commonwealth and international standards
- secrecy provisions in other legislation
- confidentiality obligations.

Structure

The guide is divided into three parts:

- **Part 1** introduces the key concepts discussed throughout these guidelines, including IPP 4, the VPDSF and VPDSS, and the relationship between privacy and security.
- **Part 2** outlines some of the factors that influence what steps may be considered reasonable, and looks at the range of steps that organisations may take to protect personal information, based on good governance practices and the four security domains outlined in the standards.
- **Part 3** contains a set of principles, which are the overarching requirements that must be in place to meet protective data security requirements.

A glossary of key terms is included at the end of this document to give definition to key concepts.
Part 1: Protection of personal information under the Privacy and Data Protection Act 2014

The Privacy and Data Protection Act 2014 (PDPA) is designed to protect all information obtained, received or held by the Victorian public sector. Parts 3, 4 and 5 of the Act respectively include obligations to protect personal information, public sector data, and law enforcement data. Both public sector data and law enforcement data may also include personal information, making the requirement to protect the security of personal information a consistent theme across the PDPA.

Information Privacy Principle 4

The PDPA contains 10 principles that govern the collection and handling of personal information in the Victorian public sector.IPP 4 – Data Security – requires organisations to protect the personal information they hold across its lifecycle – from the time it is collected until it is disposed of.

IPP 4 contains two sub-sections:

• IPP 4.1 – an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

• IPP 4.2 – an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

The key terms contained in IPP 4.1 are defined as follows:

• Hold: an organisation is taken to 'hold' personal information "if the information is contained in a document that is in the possession or under the control of the organisation, whether alone or jointly with other persons or bodies, irrespective of where the document is situated, whether in or outside Victoria". In an outsourcing context, each organisation that has control of personal information will have obligations under IPP 4.1; organisations cannot contract out of the IPPs.

• Misuse: personal information is misused if it is used in a way that contravenes the IPPs, namely, IPP 2 – Use and Disclosure. Organisations should also be aware of other restrictions around how personal information is used, such as provisions in other legislation that require confidentiality or secrecy, or internal policies that prescribe appropriate uses of information.

• Loss: personal information is lost where its physical whereabouts is unknown (including both hard and soft copy formats), or there has been a failure to preserve or maintain it. Information that has been intentionally destroyed or de-identified will not constitute a loss.

• Unauthorised access, modification and disclosure: accessing information involves viewing it in some form; modification refers to changing, removing or adding components to the original information; and disclosing information involves making it accessible or visible to others. Access, modification or disclosure of information will be regarded as 'unauthorised' where an individual has no authority to access, modify or disclose the information; exceeds their authority by acting beyond their power; or misuses their authority in pursuit of an ulterior motive.

---

2 The IPPs are contained in Schedule 1 of the Privacy and Data Protection Act 2014.
3 Section 4, Privacy and Data Protection Act 2014.
4 Office of the Australian Information Commissioner, APP Guidelines, p. 4.
Victorian Protective Data Security Framework and Victorian Protective Data Security Standards

Part 4 of the PDPA requires the Commissioner for Privacy and Data Protection to develop the Victorian Protective Data Security Framework for monitoring and assuring the security of public sector data.

The VPDSF is the overall scheme for managing protective data security risks in Victoria, and encourages a security risk management capability across the public sector. The VPDSF is underpinned by a risk-based approach to security that requires organisations to consider their operating environment and the risks they need to protect against in developing their approach to security.

The Commissioner may – and has – issued protective data security standards consistent with the VPDSF. The standards set out the mandatory security requirements for the protection of all public sector data, which includes personal information. The standards cover governance and the four security domains: information, personnel, ICT and physical security. They promote consistency in the protection of public sector data throughout the entire information lifecycle, including information sharing between organisations and with external parties.

While compliance with each of the standards is mandatory for those organisations covered by Part 4 of the PDPA, the approach that is taken to implementing the standards will differ between organisations. It is up to individual organisations to determine the most effective steps for them to take to meet the intent of each standard.

Risk-based security and ‘reasonable steps’

A risk-based approach to protective data security is reflected in both the VPDSS and IPP 4.1. Both are non-prescriptive in the way they require organisations to uphold protective data security. They afford organisations the flexibility to select the security measures and controls that are appropriate to the circumstances and to the risks they have to manage.

---

5 Sections 86(1) and (2), Privacy and Data Protection Act 2014.
Determining what steps are ‘reasonable’ under IPP 4.1 will largely be informed by risk. Risk is a dynamic concept. As risks in the organisational environment change, so will the steps that are ‘reasonable’ to effectively manage those risks and offer an acceptable standard of protective data security. For example, if an organisation chooses to move from a hard copy-based filing system to an electronic one, different security risks will emerge. As such, the steps that may have been ‘reasonable’ to protect information stored physically in hard copy format, will no longer be ‘reasonable’ in an electronic environment.

Relationship between information privacy and protective data security

Privacy and security are entwined concepts. An individual’s information privacy cannot be ensured without there being proper security in place to protect personal information from being handled inappropriately. The PDPA acknowledges this intersection, bringing together the existing information privacy regime with protective data security under a single legislative framework.

Protective data security is based on three key security attributes – confidentiality, integrity and availability – each of which must be maintained in order to achieve a reasonable level of security. Often known as the CIA triad, these three attributes are the security equivalent of the commonly used phrase for encapsulating the objective of information privacy – ‘the right information, to the right people, at the right time’.

The elements of the CIA triad are:

- **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.
Part 2: Reasonable steps for protecting personal information

This section of the guidelines introduces the security measures that may be considered ‘reasonable’ for protecting personal information.

Factors affecting what is ‘reasonable’

The security measures that are ‘reasonable’ for one organisation may not suit the requirements of another. The below factors should be taken into consideration when determining which steps to take to protect personal information.

Nature of the organisation

The characteristics of an organisation will influence the type of security measures that it should, and can, put in place to protect personal information. Some of the relevant organisational factors include:

- what information assets it obtains, receives or holds, and the value\(^6\) of that information
- the risk appetite and tolerance of the organisation
- the size of the organisation
- the resources it has at its disposal, including financial and personnel
- its business model and the nature of its operations – for example whether or not it is customer-facing
- any outsourcing arrangements that may be in place
- any other security requirements that the organisation is required to take into account – for example Payment Card Industry Data Security Standards (PCI-DSS) and Australian Standards.

Type and amount of information held

The type and value of the information itself will influence the protective data security measures that are required to protect an organisation’s information. For example, sensitive information may require more stringent security measures than other types of information, given the greater risk of harm to individuals if the confidentiality, integrity or availability of this information were compromised.

The more personal information an organisation holds, the risk that accompanies this information will also increase. Organisations may need to take additional steps to protect large, aggregated information holdings such as large electronic databases.

Potential impact of a privacy breach

The security measures that are put in place should be proportionate to the potential consequences – to both the organisation and to individuals – if the confidentiality, integrity or availability of the information were compromised.

Citizens have an expectation that their privacy will be protected when they provide their personal information to a government organisation. As such organisations must be cognisant of the potential consequences that individuals may face if a privacy breach were to occur, and protect the information

---

\(^6\) The term ‘value’ with respect to information is discussed further on page 12.
they hold accordingly. Some of the potential consequences to an individual could include financial or reputational harm, embarrassment, discrimination, and even a threat to their safety or wellbeing.

The risks to the organisation itself in the event of a security breach should also be considered when looking to implement security measures. The likely consequences of losing public trust, financial and reputational damage, as well as adversely affecting stakeholder relationships should encourage robust protective data security practices.

Privacy invasiveness of security measures

In some cases, security measures that are designed to protect individuals’ privacy may be privacy-invasive in themselves. For example, requiring employees to swipe an access card for entry into their workplace may be considered reasonable to protect against unauthorised access to a restricted area. Requesting staff to provide their fingerprint for authentication however may be intrusive and unreasonable in this situation. The effect of security measures must be balanced against the value of the information and the business objective they are trying to support.

The Charter

All Victorian public sector organisations are bound by the Charter of Human Rights and Responsibilities Act 2006 (the Charter), which comprises 20 human rights that all individuals should be afforded. The Charter makes it “unlawful for a public authority to act in a way that is incompatible with a human right or, in making a decision, to fail to give proper consideration to a relevant human right”. When considering how to best protect personal information, organisations must give due consideration to human rights and ensure that any measures they implement do not interfere with the rights of individuals.

Reasonable steps for protecting personal information

The ‘reasonable’ steps outlined in this section are based on good governance practices and the four security domains:

- information security
- personnel security
- ICT security
- physical security.

Each of these domains speaks to important concepts that underpin the protection of personal information. No protective data security framework is complete without incorporating measures that cover each of the domains.

---

Organisations must ensure that wherever personal information travels, security measures travel with it. When information moves within an organisation, between different formats, or is shared with other organisations, the security measures that were applied at the source of the information need to be respected and an equivalent level of assurance maintained.

Governance

The Australian Government Protective Security Policy Framework describes protective security governance as being about how an agency manages its conformance with its security obligations, and how it uses security arrangements to contribute to its overall performance. Good security governance is underpinned by executive support, an essential starting point for the protection of personal information.

Security management framework

To ensure the protection of personal information, organisations should have in place an overarching security management framework that provides a foundation for the organisation’s security direction. An organisation’s approach will be proportionate to its size, resources and risk posture.

A security management framework should clearly define key roles, responsibilities, accountabilities and authorities for positions that are tied to security governance. It is critical that executive support and approval for a security management framework is obtained, to ensure that each party involved in security management has the support to effectively undertake their role. A security management framework should also be widely communicated both internally and externally to relevant stakeholders, to ensure that those who influence the effectiveness of the framework – and those who will be affected by the framework – understand its key objectives.

Security risk management

As part of a security management framework, organisations should define their approach to assessing and managing security risks. An organisation’s risk appetite and tolerance will inform the approach taken to managing risks. These may change over time, pursuant to internal and external organisational factors, and as such it is important to continually reassess risks. This includes regular reviews to address the changing environment, and a consideration of any new information that had not been previously accounted for.

Security policies and procedures

Policies and procedures are an essential component of a robust security management framework. These documents should be widely communicated, and made easily accessible to all persons. Policies and procedures are crucial for ensuring that individuals are aware of their obligations and responsibilities, and understand any legislative obligations by which the organisation may be bound.

Training and awareness

Security awareness training must be embedded into organisations’ induction programs; even where individuals are not expected to directly handle personal information as part of their role, it is important that they are made aware of the organisation’s privacy and security obligations generally. Training should not be seen as a one-off exercise, but should be reinforced at regular intervals, particularly where significant changes to the regulatory or legal environment affect the organisation’s security obligations.

Training is critical for minimising the risk of human error, which is one of the major causes of privacy and security breaches.9 Security training should involve making individuals aware of:

• the security policies and procedures that must be followed
• any specific security responsibilities they have that are tied to their roles or functions
• what information they can and cannot access, tied to the need-to-know principle
• who within the organisation is accountable for security risk management
• security incident reporting processes.

Business continuity

Ensuring that an organisation’s core business is able to sustain a disruption to normal business practices is a critical element of good governance.10 A business continuity plan consists of policies and programs that outline how the organisation will continue to carry out its functions in the event that its critical infrastructure (including information), people and processes are negatively impacted. This enhances organisational capacity to respond to, manage and recover from unexpected events that threaten core business, and builds resilience against future threats.

Business continuity management should feature as a key component of a security management framework, to strengthen the position of organisations to uphold reasonable security when information assets and information infrastructure are threatened. The plan should be regularly tested, reviewed and updated.

Security incident management

Even where precautions are taken to prevent a compromise to the confidentiality, integrity and availability of information, security incidents still occur. As such, organisations should have in place an incident management regime for preparing for, and responding to security incidents in a timely manner. The required steps include:

• Preparation: establishing a security incident management scheme, supporting organisational awareness and training of security obligations, and strengthening organisational incident management capabilities.
• Detection: robust incident detection capability, integrated with systems and processes to support the timely detection of security incidents.
• Handling: consistent incident assessment processes to categorise and prioritise incidents.
• Prevention: undertake post incident analysis of causes and handling of each incident; implementation of improvements based on lessons learnt; and review, validation and update of the security incident management scheme.11

---

9 Office of the Australian Information Commissioner, Guide to securing personal information: ‘Reasonable steps’ to protect personal information, 2015, p. 18.
11 The former Office of the Victorian Privacy Commissioner produced guidelines for responding to privacy breaches, which should inform the steps that organisations take in the event that a breach does occur. These guidelines and an accompanying checklist can be accessed at https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-guidelines.
External party engagement and oversight

Protective data security obligations under IPP 4.1 also extend to contracted service providers who provide a service on behalf of a public sector organisation under a state contract. When outsourcing to third parties, organisations must ensure that privacy and security obligations are reflected in contractual arrangements.

For instance, any contracts should clearly define the roles and responsibilities of each party, including who ‘owns’ the information and who is accountable. This includes detailing specific responsibilities in the case of a privacy breach.

Organisations should also ensure that contracts include review mechanisms, so that the outsourcing organisation can monitor third party compliance with the terms of the arrangement, and amendments can be made if required. Accountability for security cannot be outsourced.

Information security

Information security broadly considers the protection of information throughout its entire lifecycle, from the time that information is collected through to the point of disposal. This means that security measures need to be incorporated at every stage of the information lifecycle, taking into account the changing value of the information. The steps that organisations should take to protect information apply irrespective of the form the information takes, whether it is soft or hard copy material.

Information value

In order to apply the appropriate security measures to protect personal information, organisations must first understand the value of that information.

‘Value’ refers to the overall importance of the information, which organisations can determine by considering the potential impacts to the confidentiality, integrity and availability of the information if it were compromised. Once the value of the information has been determined, organisations can then apply commensurate security measures to protect the information.

The application of a protective marking is one such security measure. Protective markings act as an important visual signal to anyone accessing the information, indicating the minimum security controls to be applied during the use, handling, storage, transfer and disposal of the information.

Information sharing

Prior to sharing personal information, organisations should ensure that security measures are part of information sharing arrangements. These security measures need to address governance and the core security domains of information, personnel, ICT and physical security, and must be applied at each stage of the information sharing process. Agreements – which can take the form of memoranda of understanding or information sharing agreements – should be actively managed for relevance and currency, to ensure they are meeting their intended purpose.

By implementing security measures for information sharing, organisations ensure that the objective of information privacy is maintained – the right information, to the right people, at the right time.

---

12 Section 17(2), Privacy and Data Protection Act 2014.
14 CPDP has published guidelines for sharing personal information in the Victorian public sector, which specifies what should be included in an information sharing agreement, and further describes the privacy and data security considerations that need to be taken into account when sharing personal information. The guidelines are available at https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-guidelines.
Personnel security

The intention of personnel security is to ensure that access to official information is only granted to those individuals who are eligible and suitable. By employing personnel security measures, organisations seek to reduce the risk that information will be compromised. Personnel security also contributes to creating a protective security culture, in which those who access information are aware of their security responsibilities and understand the value in upholding good security practices.¹⁵

Pre-employment screening

As part of the recruitment process, organisations should establish pre-employment screening measures to ensure that candidates meet the minimum personnel security requirements, prior to being made an offer of employment.

Employers should clearly define eligibility or suitability requirements for their organisation that candidates need to meet, and communicate these to candidates during recruitment. This may include advising potential applicants of what screening measures will be conducted, such as a national criminal record check or checks for a security clearance. Screening measures may differ depending on the specific role and their access to particular information within an organisation.

Ongoing personnel security management

Personnel security also forms an important basis for an organisation’s ongoing security management regime. For instance, organisations should have the proper processes in place to manage:

- the ongoing eligibility and suitability of employees
- access arrangements to sensitive information,¹⁶ which may include interim, short term and ongoing access
- active assessment of personnel risks
- non-compliance with security obligations or staff misconduct
- staff departures from the organisation.¹⁷

ICT security

The purpose of ICT security is to ensure that information communication and technology systems that process and store information have adequate security measures in place. With a growth in the digitisation of information assets, ICT security measures are critical in enabling organisations to meet their business objectives whilst maintaining the confidentiality, integrity and availability of information.


¹⁶ Sensitive information may refer to either sensitive (personal) information as defined in Schedule 1 of the Privacy and Data Protection Act 2014, or information that has been given a ‘sensitive’ security classification.

ICT system lifecycle

Organisations must take steps to protect both hardware and software from misuse, loss, and unauthorised access, modification or disclosure. ICT security extends to platforms including email systems, desktop and portable devices (such as laptops, mobile phones, tablets and portable storage devices), websites and social media, Wi-Fi networks, and remote access capabilities.18

In order to secure ICT systems, organisations should apply security measures throughout the system lifecycle, from initial planning, design and development, through to implementation, and subsequent decommissioning.

To assist organisations in prioritising their efforts, the Australian Signals Directorate (ASD) has devised four strategies – known as the ASD Top 4 – to help mitigate threats to ICT systems. By doing so, organisations reduce the risk of an incident compromising personal information.

The ASD Top 4 requires organisations to:

- **Whitelist**: application whitelisting is a technical measure that only allows permitted applications to run on a system, preventing malicious software and unauthorised applications from running.
- **Patch applications**: applications should be patched to fix problems and update software to the latest versions, as out-dated applications are more vulnerable to a malicious attack.
- **Patch operating systems**: operating systems also need to be kept up to date, as newer versions are designed with greater security protections built in. Timeliness is crucial when patching systems, to reduce the window of opportunity that intruders have to exploit a known vulnerability in an operating system.
- **Restrict administrative privileges**: administrative access to ICT systems should be limited only to those employees that require it to perform their role, as malicious intruders are more likely to target these accounts given their high level of access to systems.19


Physical security

Organisations must take steps to prevent unauthorised access to personal information that could be exposed as a result of poor physical security. To achieve this, they must ensure that security measures are integrated into facilities, equipment and services designed to protect information.

Physical security lifecycle

Physical security lifecycle requires organisations to establish, implement and maintain physical security measures commensurate to the type and value of the information they hold. This approach requires organisations to provide a secure environment where hard copy (physical files) and soft copy (electronic documents) information is adequately protected.

Measures may include:

- **Facilities**: designing specialist work spaces where sensitive information can be segmented off to only permit access to those who have the appropriate authorisation, and maintaining access logs to monitor staff movements within the physical environment.20

---

• **Equipment**: selecting security equipment to protect information during use or transfer (such as satchels, tamper evident bags, locked briefcases), ensuring secure containers are available for information to be locked away, and supporting clear desk policies.

• **Services**: monitoring and patrol of physical spaces, for example with security guards or live monitoring of security camera feeds.

The above security measures highlight the need for organisations to implement multiple layers of security that work together to protect information. Any single security measure, without the appropriate maintenance and support, will not effectively protect information.

Applying physical security measures is not a one off exercise, but must be continually monitored, evaluated, and improved to account for changes in the physical and regulatory environments, and the organisation’s risk appetite and tolerance. This ensures that the security measures that are in place are effective and are meeting their objective.
Part 3: Underlying principles for protecting personal information

There are a number of principles that should guide organisations in deciding how best to manage protective data security throughout the information lifecycle. The principles outlined below are drawn from the guiding principles of the VPDSF.

**Governance**

Governance is one of the most important foundational principles for protective data security. Public sector governance is about how an organisation is managed, its organisational structures, its culture, the policies and strategies that guide the organisation, and the way it manages its various stakeholders. Robust governance arrangements that support the protection of personal information should be implemented at the outset – before any personal information is collected – to minimise the potential for a security breach.

Organisations must ensure they have in place:

- proper oversight and monitoring, which is essential to ensuring that policies and procedures are in place to guide daily organisational practices, and that they are effective at achieving their purpose
- clearly defined lines of accountability, responsibility and leadership, so that all employees – and in some cases external parties – are aware of who within an organisation maintains responsibility for strategic direction, compliance, incident management etc.

**Risk management**

Too often it takes an incident that negatively impacts an organisation for senior executives and leaders to take an interest in protective data security. A risk management approach to protective data security is critical for proactively identifying, evaluating and managing risks upfront, rather than waiting for an incident to arise before responding to mitigate adverse consequences.

As a matter of good practice and in line with the Victorian Government Risk Management Framework, organisations should implement a risk management framework that sets out the foundational components for designing, implementing, monitoring, reviewing and continually improving risk management. Ongoing risk assessments are a critical component of a risk management framework to ensure that organisations are equipped to respond to new and changing threats and vulnerabilities. A risk-based approach to implementing security measures supports a flexible, tailor-made solution to managing protective data security risks, rather than traditional compliance-based models of security.

Examples of the types of risk management strategies that organisations can use include:

- Privacy by Design, which is a methodology for ensuring that good privacy practice is embedded into business activities and projects from their inception
- privacy impact assessments, which assess an organisation’s compliance with core privacy principles in respect of a particular project or program

---

23 Privacy by Design is a concept developed by Dr Ann Cavoukian, former Information and Privacy Commissioner of Ontario. CPDP has produced a background paper on Privacy by Design and its application in the Victorian public sector, available at: https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-background-papers.
• security risk assessments, including security risk profile assessments (SRPAs) and protective data security plans (PDSPs).25

**Information value**

Central to being able to protect personal information is understanding its value. Determining the value of information requires an assessment of the potential impacts if the confidentiality, integrity or availability of the information were compromised. For example, organisations must consider the potential impacts if personal information were to fall into the hands of an individual who is not authorised to access it.

Once the information value is ascertained, the appropriate security measures can be applied. The VPDSF contains resources that will assist organisations to assess the overall value of their information assets.

**Security culture**

An organisation's culture is underpinned by its leadership, values and norms, and influences the day-to-day activities and behaviours of its staff. For organisations to effectively implement the necessary security measures to protect the information they hold, a knowledge and appreciation of security practices must be embedded into organisational culture. This can foster a shared understanding and responsibility for the protection of information and management of risk across the organisation.

To affect cultural change, organisations must build protective data security practices into everyday operations, and instil a shared responsibility for security in all employees.

**EVERYONE’S RESPONSIBILITY**

**Continuous improvement**

A key protective data security concept is the continuous improvement lifecycle. Implementing protective data security measures is not a one off task, but requires ongoing monitoring and improvement to respond to changing environments and ensure that those security measures continue to meet their intended objectives.

The VPDSF promotes a *plan, do, check, act* methodology, requiring organisations to:

• understand the business and its core functions, and plan accordingly
• integrate security measures that are proportionate to business risks
• undertake monitoring and assurance activities to ensure that implemented security measures meet business objectives while minimising business risks
• review, validate and update based on business objectives, risks, and operations based on lessons learnt.

---

25 See the VPDSF for more information on SRPAs and PDSPs.
Business objectives

Protective data security practices are integral to enabling organisations to meet their business objectives in an efficient, effective and economic way. The information an organisation holds is one of its most critical assets, and reliable information is central to enabling organisations to undertake their functions and deliver value to the community. Having confidence in information requires that the core attributes – confidentiality, integrity and availability – be maintained, through implementing appropriate protective data security measures.
Summary

The responsibility for protective data security does not solely rest with an organisation’s security and privacy experts, but requires a consolidated effort by all staff. Despite common perception, protecting information does not only equate to the implementation of ICT security measures – it extends far beyond that. The establishment of good governance practices, securing the information throughout its lifecycle, engaging the right personnel, and securing physical environments are important security measures that work hand in hand. Organisations must be mindful that the protection of personal information requires buy-in and support at an executive level, as well as whole of business engagement drawing on legal, finance, information management, ICT, policy and human resources.

The IPPs and the VPDSS do not take a prescriptive approach in directing organisations how to protect personal information. Rather they are designed to enable organisations to decide for themselves the most appropriate steps to protecting the personal information they hold, proportionate to the value of their information, and the organisation’s size, risks and resources.

To assist organisations in effectively meeting their IPP 4.1 obligations, these guidelines have outlined some of the steps that may be ‘reasonable’ for organisations to take when protecting personal information from misuse, loss, and unauthorised access, modification or disclosure. The guidance in this document is non-exhaustive, and every organisation will approach protective data security in a different way. Organisations bound by Part 4 of the PDPA may have additional considerations under the VPDSF and the standards that need to be accounted for in addition to those steps taken under IPP 4.1.

Further advice and guidance is available in the VPDSF or from the CPDP Data Protection branch.
<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The desired state that allows authorised persons to access defined information for authorised purposes at the time they need to do so.</td>
</tr>
<tr>
<td>Charter of Human Rights and Responsibilities (the Charter)</td>
<td>Sets out the basic human rights, freedoms and responsibilities of all people in Victoria. The Charter requires public authorities and people delivering services on behalf of the government to act consistently with the human rights in the Charter.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>The limiting of official information to authorised persons for approved purposes. The confidentiality requirement is determined by considering the potential consequences of unauthorised disclosure of the official information.</td>
</tr>
<tr>
<td>Contracted service provider</td>
<td>A person or body who provides services under a state contract.</td>
</tr>
<tr>
<td>Governance</td>
<td>How an organisation is managed, its organisational structures, its culture, the policies and strategies that guide the organisation, and the way it manages its various stakeholders (derived from the Australian National Audit Office).</td>
</tr>
<tr>
<td>Information lifecycle</td>
<td>The use and management of official information from cradle to grave.</td>
</tr>
<tr>
<td>Information privacy</td>
<td>Refers to an individual's right to determine for themselves who has access to their personal information and how it is used.</td>
</tr>
<tr>
<td>Information Privacy Principles (IPPs)</td>
<td>Refers to the 10 principles contained in Schedule 1 of the Privacy and Data Protection Act 2014 that set out the minimum requirements for the collection and handling of personal information in the Victorian public sector.</td>
</tr>
<tr>
<td>Information sharing</td>
<td>Describes the process of disclosing information from one party to another, who subsequently collects that information.</td>
</tr>
<tr>
<td>Integrity</td>
<td>The assurance that official information has been created, amended or deleted only by the intended authorised means and is correct and valid.</td>
</tr>
<tr>
<td>TERM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Law enforcement data</td>
<td>Any information obtained, received or held by the police force of Victoria for the purpose of its law enforcement functions or activities.</td>
</tr>
<tr>
<td>Organisation</td>
<td>A body to which Part 3 of the Privacy and Data Protection Act 2014 applies as defined in section 13 of that act.</td>
</tr>
<tr>
<td>Personal information</td>
<td>Defined in the Privacy and Data Protection Act 2014 as information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies.</td>
</tr>
<tr>
<td>Privacy and Data Protection Act 2014</td>
<td>Victorian legislation that is designed to protect all public sector data, including personal information and law enforcement data.</td>
</tr>
<tr>
<td>Privacy by Design (PbD)</td>
<td>A methodology that enables privacy to be ‘built in’ to the design of information systems and business processes, ensuring that privacy is considered before, and throughout, the development and implementation of all initiatives that involve personal information.</td>
</tr>
<tr>
<td>Privacy impact assessment</td>
<td>A tool used to assess an organisation’s compliance with their information privacy obligations and requirements, and to identify any potential privacy risks that may arise if an initiative was to be implemented in its current form.</td>
</tr>
<tr>
<td>Protective data security</td>
<td>A risk management process designed to safeguard official information assets and services in a way that is proportionate to threats and supportive of business; uses a combination of procedural, physical, personnel, information and ICT security measures to protect against security threats (also referred to as data protection or information security).</td>
</tr>
<tr>
<td>Protective marking</td>
<td>An administrative label assigned to official information that is directly linked to the business impact level for a potential compromise of its confidentiality. It also informs the minimum protection requirements during use, storage, transmission, transfer and disposal.</td>
</tr>
<tr>
<td>Public sector data</td>
<td>Any information (including personal information) obtained, received or held by an agency or body to which Part 4 of the Privacy and Data Protection Act 2014 applies.</td>
</tr>
<tr>
<td>TERM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>The type and amount of risk that an organisation is prepared to accept or avoid (derived from the Victorian Government Risk Management Framework).</td>
</tr>
<tr>
<td>Risk posture</td>
<td>An organisation’s overall risk position, that is, current business and strategic risks being managed.</td>
</tr>
<tr>
<td>Risk profile</td>
<td>A description of any set of security risks for an organisation, relating to either the whole organisation or part of the organisation.</td>
</tr>
<tr>
<td>Risk tolerance</td>
<td>An organisation’s readiness to bear the risk after risk treatment in order to achieve objectives. Risk tolerances are based on the maximum level of acceptable risk and may be expressed in various ways depending on the nature of the risk (derived from the Victorian Government Risk Management Framework).</td>
</tr>
<tr>
<td>Security domains</td>
<td>Refers to key areas of information, ICT, personnel and physical security.</td>
</tr>
<tr>
<td>Security measures</td>
<td>A policy, procedure or technical solution for mitigating security risks and protecting information.</td>
</tr>
<tr>
<td>Security risk profile assessment</td>
<td>A forma endorsed document that identifies an organisation’s protective data security risks under the Victorian Protective Data Security Framework.</td>
</tr>
<tr>
<td>Value</td>
<td>The overall business impact of information, based on an assessment of compromise to the confidentiality, integrity, or availability of the information. The value of information informs the security measures needed to protect it.</td>
</tr>
<tr>
<td>Victorian Protective Data Security Framework</td>
<td>The overall scheme for the security of Victoria’s public sector data, as required under section 85 of the Privacy and Data Protection Act 2014.</td>
</tr>
<tr>
<td>Victorian Protective Data Security Standards</td>
<td>18 standards that cover governance and the four security domains for the security, confidentiality and integrity of public sector data and access to public sector data. The standards form part of the Victorian Protective Data Security Framework.</td>
</tr>
</tbody>
</table>