Office of the Victorian Information Commissioner

IPP 4 – Data Security

Freedom of Information | Privacy | Data Protection

IPP 4 – Data Security

On this page

4.1 IPP 4 contains two distinct obligations. The first deals with data security, requiring organisations to protect personal information they hold. The second deals with the disposal of data, requiring organisations to destroy or de-identify personal information they no longer need. IPP 4 says:

> 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.

IPP 4.1: Security of personal information

4.2 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 and disclosure. To comply with IPP 4.1, organisations should anticipate foreseeable security risks to the personal information they hold and take reasonable precautions to protect the information from those risks.

4.3 When determining whether a particular step is 'reasonable', organisations must consider the potential impact of a possible security breach of the information on the people the information is about. As explained in the Key Concepts chapter, what is reasonable depends on the circumstances. The requirement to take reasonable steps supports a risk-based approach to the security of personal information.

4.4 IPP 4.1 is particularly concerned with the potential harm caused to an individual if the security of their personal information is compromised. Potential harm to an individual may include financial or reputational harm, embarrassment, discrimination, a threat to their safety or wellbeing. This means IPP 4.1 requires an organisation to implement measures proportionate to the potential privacy risks to individuals and the potential harm caused to them.

4.5 IPP 4.1 and Parts 4 and 5 of the PDP Act support a risk-based approach to implement measures proportionate to their respective risks. However, unlike IPP 4.1, Part 4 focuses on information security, rather than the privacy of personal information. Some of the security measures implemented as part of managing information security risk may be useful to assist organisations in protecting the personal information they hold.

4.6 'Reasonable' information security measures should be identified and implemented based on the outcomes of a risk assessment conducted on the organisation's information assets.[1] This risk-based approach gives organisations flexibility to select and tailor security measures and controls specific to the circumstances and risks they have to manage. Because risk is dynamic and will change when the organisation's information practices change – for example, when new technologies are adopted or

[1] The assessment considers the impacts to the organisation if there were a compromise of the confidentiality, integrity and availability of its information assets.

staff responsibilities change – organisations should periodically review their information security risks and assess if the steps they take to manage those risks remain 'reasonable'.

4.7 If a Victorian public sector organisation fails to take 'reasonable steps', it breaches IPP 4.1. The discussion about IPP 4.1 in this section of the Guidelines is divided into three parts:

a. The first part, 'Determining whether a security measure is required by IPP 4', outlines factors relevant to determining whether a certain 'step' is required by IPP 4.1. This discussion will be useful when an organisation is considering implementing particular information security measures or responding to a privacy complaint that alleges a failure to implement a *particular* security measure amounts to a breach of IPP 4.1. The organisation might be asking itself: would that particular security measure have been reasonable? May we have breached IPP 4.1 by deciding not to implement that measure?

b. The second part, 'Implementing a suite of security measures to protect personal information', explains how to identify a range of security measures to protect personal information held by the organisation. Certain Victorian public sector organisations should apply the Victorian Protective Data Security Framework (**VPDSF**). This complements the identification and implementation of security measures under IPP 4.1. This part might be useful to organisations when designing information management systems or re-designing them after a privacy complaint about the 'reasonableness' of their security measures.

c. The third part explains certain key terms used in IPP 4.1: hold, misuse, loss and unauthorised access, modification and disclosure.

Determining whether a security measure is required by IPP 4: 'Reasonable steps'

4.8 Perfect security is impossible. No organisation will be able to implement all possible security measures to mitigate all risks to the information it handles. This is why IPP 4.1 only requires organisations to take reasonable steps to secure personal information.

4.9 When considering whether a particular step is reasonable, and required by IPP 4.1, the main consideration is the risk of harm to the people the information is about. Other considerations include the cost and difficulty of implementing the security measure and the damage to the organisations that might result from a failure of security or a breach. In the context of IPP 4, a 'failure of security' or 'data breach' refers to 'misuse or loss [or] unauthorised access, modification or disclosure' of personal information.[2] 'Reasonable steps' is a balancing act between these considerations. Overall, 'reasonable' security measures are those proportionate, appropriate and relevant to the risk of harm to the individual whose personal information is concerned.

4.10 Organisations can consider the following factors when determining whether a particular security measure is 'reasonable':[3]

- the potential impact of a breach or security failure, such as a compromise to the confidentiality or integrity of personal information;
- the likelihood of the breach occurring;
- the type and amount of personal information;
- the nature of the organisation and difficulty of implementing the step;

[2] See IPP 4.1 in Sch 1 of the PDP Act.
[3] The Australia Law Reform Commission (**ALRC**) lists similar factors: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108, August 2008), Recommendation 28-3.

- the invasiveness of the security measure; and
- other negative consequences of implementing the 'step' (including any adverse impact it may have on the availability of the information to its intended user).

The potential impact of a security breach

4.11 As noted above, when assessing the 'reasonableness' of the steps that organisations intend to implement, organisations need to consider the potential harm to individuals which could arise from a breach of their personal information.

4.12 In assessing the potential harm, organisations should be mindful of the gravity or severity of this harm. The severity of harm might vary depending on who receives the information as result of a breach. For example, if a breach results in a colleague knowing a certain piece of personal information about a fellow colleague, the effect on the individual with regard to embarrassment, humiliation or discrimination might be different to if a family member were to discover the same information. Harm can also follow from a breach that compromises the integrity of information. For example, if a person's record is improperly modified to incorrectly state that the person is in debt, and this affects their ability to obtain finance, this can be as harmful as an unauthorised disclosure of personal information.

The likelihood of a security breach occurring

4.13 If a security breach has occurred and organisations are consulting these guidelines to determine if their security measures were reasonable or not, organisations could ask themselves:

- How likely was the security breach?
- Should it have been foreseen?
- Were the security measures in place proportionate and appropriate to how likely the security breach was?

4.14 These questions should help an organisation reflect on the reasonability of its 'steps' to securing the information.

The type and amount of the personal information

4.15 The type and sensitivity of the personal information will affect what is reasonable to protect it from misuse or loss, or unauthorised access, modification or disclosure. There is a greater risk of more serious harm to individuals if the security of sensitive information is compromised. This means sensitive information may require more enhanced security measures than other types of information. For example, sensitive information such as racial or ethnic origin can be used to discriminate. Also, unauthorised access to financial information may risk identity fraud or financial harm.

4.16 The amount of information may also be a factor for organisations to consider when deciding if their 'steps' were reasonable. This is also a relevant consideration when deciding whether or not to notify an individual their information has been compromised. The amount of personal information held by an organisation that could potentially be the subject of a security breach could also affect the severity of the impact on the individual. If the amount of personal information can build a detailed profile of an individual, the risk of harm caused by a breach will be greater, for example, through identity theft. If the information is such that it can be linked with other information to draw a detailed picture about an individual, this may also heighten the value of the information.

4.17 For a detailed discussion of the risks of linking unit-level records of information and re-identification making information 'personal information', see OVIC's report 'Protecting unit-record level personal

information'. For a high-level overview of de-identification in the context of unit-level data, see OVIC's 'De-identification and Privacy Background Paper'.

4.18 Organisations may also wish to refer to the Business Impact Level (BIL) table issued as part of the Victorian Protective Data Security Framework to consistently assess the potential impact of an information compromise.

The nature of the organisation and difficulty of implementing the 'step'

4.19 The nature of an organisation influences what constitutes a 'reasonable step'. Specifically, the resources available to an organisation to implement security measures and the cost of implementation will affect what is 'reasonable'.[4] Organisations implementing 'reasonable steps' must also be able to continue their normal business practices. The size, capabilities and budget of an organisation to implement security 'steps' is a consideration which may weigh against the likelihood and severity of harm that may be caused to an individual whose information is the subject of a security breach.

4.20 However, it should be noted that a lack of resources is not a defence that should be relied on if the organisation deliberately undertook to collect information, even though it had no reasonable mechanisms for securing it.

4.21 Specifically, organisations may consider the difficulty of implementing the security measure. A time-consuming and costly 'step' might not be 'reasonable' if the potential harm to an individual from a security breach is limited. Security measures might be difficult or costly to implement if, for example, they require a complete redesign of the digital information software management programs. While information management systems should be designed with privacy in mind,[5] the 'reasonable' part of IPP 4.1 recognises organisations cannot have perfect information security: the time and cost involved with implementing the security measure may not be proportionate and appropriate to the risk of a breach.

4.22 This consideration must be taken into account in the context of IPP 4.1: its aim is to protect the personal information of individuals. This means the harm to individuals is *the most important consideration*. A difficult or costly security measure might be 'reasonable' if it is proportionate to the risk of harm, for example, if the organisation deals with particularly sensitive information.

The invasiveness of security measures

4.23 In some cases, security measures designed to protect individuals' privacy may be privacy-invasive themselves. A factor for determining reasonable steps for information security is the 'privacy infringements that could result from such data security steps'.[6] For example, requiring employees to swipe an access card for entry into their workplace may 'reasonably' protect against unauthorised access to a restricted area, however, requesting staff to provide their fingerprint for authentication may be intrusive and unreasonable. In *Jeremy Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946, the Fair Work Commission found the requirement by an employer of an employee to submit to the

---

[4] The ALRC suggests 'cost of implementation' is a factor for reasonable steps for data security. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108, August 2008), Recommendation 28-3.

[5] A Privacy Impact Assessment (**PIA**) can help organisations design information handling processes and procedures with privacy in mind. Additionally, see 'Privacy by Design: Effective privacy management in the Victorian public sector', a 2016 background paper by OVIC's predecessor, the Commissioner for Privacy and Data Protection (**CPDP**).

[6] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108, August 2008), Recommendation 28-3.

collection of his fingerprint data was inconsistent with APP 3 (the collection principle equivalent to IPP 1), partly because the employer did not have a privacy policy and had not issued the employee a privacy collection notice.[7]

4.24 Any negative consequences of implementing security measures must be balanced against the risk of harm to the individual who is the subject of the information arising from a failure of security or data breach.

Other negative consequences from implementing the step

4.25 A security measure might not be a 'reasonable step' if it goes above and beyond the risks associated with the personal information. If the risk of security breach or the risk of harm to the individual caused by the breach is minimal, but the security measure severely limits access to that information, the availability of that personal information might be unnecessarily restricted.

4.26 When considering if a security measure is reasonable, organisations might find it helpful to think about the three themes of the information security triad: confidentiality, integrity and availability. Confidentiality is about limiting access to information. Integrity is about preventing unauthorised modification, like IPP 3 (Data Quality). Measures designed to protect privacy can sometimes appear to be in opposition to the theme of availability of information. Information can be incredibly useful for organisations to make decisions about people. If the availability of information must be restricted to implement a security measure, such a security measure would be unlikely to be a requirement under IPP 4, if the impact of the restriction is disproportionate to the risk being managed.

4.27 When considering IPP 4.1, the *principal consideration* is the reduction of the risk of harm to individuals caused by information privacy or security breaches. The difficulty of implementing a security measure, the time and cost involved, or the reduced availability of the information are factors to be considered, as are the negative consequences for the organisation are valid concerns, but the protection of the information and the individual is paramount.

Implementing a suite of security measures to protect personal information

4.28 How can an organisation identify the appropriate security measures for their organisation to meet the requirement of 'reasonable steps' under IPP 4.1? This process will involve multiple 'steps' which should involve controls across all security areas: governance, information, personnel, ICT and physical. Thinking about all security areas should help organisations select a range of security controls which together build an information security program that is 'reasonable' in the organisation's context. These Guidelines explain and provide examples of security measures as part of governance, information security, personnel security, ICT security and physical security.

4.29 The Five Step Action Plan in the Victorian Protective Data Security Framework (**VPDSF**) also provides a method to identify appropriate security measures for an organisation. The VPDSF is the overall scheme for managing information security risks across the Victorian public sector. Like IPP 4.1, it is underpinned by a risk-based approach to information security. The Five Step Action Plan is ordinarily used to build a model of *the organisation's* information security risks, and measures that need to be implemented to mitigate those risks. However, the Five Step Action Plan may also assist organisations to identify the risks to *personal information* and the risk to the privacy of individuals, in accordance with IPP 4.1. Victorian government organisations should refer to the Victorian Protective Data Security Framework and Standards for more information.

[7] *Jeremy Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 [48]-[50].

4.30 The Victorian Data Protection Security Standards (**VPDSS**) require organisations to adhere to a minimum set of protective data security requirements. Like these guidelines, the VPDSS encourage organisations to consider all security areas (governance, information, personnel, ICT and physical).

The Five Step Action Plan:

1. Identify your information assets.
2. Determine the value of this information. The value is how useful the information might be to the organisation (within authorised use).
3. Identify the risks to this information. This involves the likelihood of a breach and the severity of harm to the individual should a breach occur.
4. Apply security measures to protect the information.
5. Manage risks across the information lifecycle from collection, while the information is held and when it is destroyed or de-identified under IPP 4.2.

The security areas

Governance

4.31 Appropriate privacy governance involves establishing practices, procedures and systems that ensure an organisation has appropriate governance measures in place to protect personal information. Governance measures will be most often implemented at an organisational or management level, for example, with policies on information management. Policies and procedures are an essential part of organisational governance. Policies and procedures contribute to robust security management because they help make staff aware of their obligations and responsibilities and understand any legislative obligations by which the organisation may be bound. They also promote consistency of practice by staff which means individuals can trust their information will be handled appropriately.

4.32 Organisations are encouraged to have security and privacy policies and conduct security risk assessments.

4.33 An organisational policy that requires PIAs be completed regarding projects involving personal information might be one 'step' in the organisation's approach for protecting information. PIAs often form part of an organisation's overall corporate risk assessment procedure. They help organisations identify and mitigate possible information security and privacy risks and what controls across the security areas (discussed below) it might be reasonable to implement.[8] PIAs are a major component of IPP 4.1.

4.34 Organisations should have a security policy or a security management framework that defines key roles, responsibilities, accountabilities and authorities for positions tied to security governance. For

[8] See OVIC's guidance on PIAs.

example, some organisations will already be required to submit a Protective Data Security Plan (**PDSP**) as part of the Victorian Protective Data Security Standards (**VPDSS**) and Framework (**VPDSF**). A security management framework should be widely communicated internally and externally to relevant stakeholders so those who influence the effectiveness of the framework and those who will be affected by the framework understand its key objectives. Establishing, implementing and maintaining an information security management framework that is relevant to the organisation's size, resources and risk posture is also a standard of the Victorian Protective Data Security Standards.[9]

4.35 Organisations should try to design security policies and procedures in a way that supports, rather than restricts, other IPPs. For example, a heavy focus on confidentiality should limit only unauthorised access to that information. Confidentiality should not impede an individual's ability to access and correct their own information which is a right established by IPP 6 (Access and Correction).

4.36 Training and awareness are other important parts of protecting information through governance. Strong internal guidance and training about information security promotes a security culture in the organisation. It also helps individuals understand the importance of good information handling practices.[10] Security awareness training should be embedded into organisations' induction programs and be reinforced at regular intervals, particularly where significant changes have occurred to the legal, regulatory or technological environment.

4.37 Allowing the organisation to continue normal business practices is key to 'reasonable' governance measures, provided the practices do not contravene the IPPs. This is part of the balancing act between harm to an individual from a potential security breach and the cost and difficulty for organisations to implement security controls. See the discussion of reasonable steps above, specifically at paragraphs [4.7]-[4.21].

4.38 The obligation to take reasonable steps to protect personal information under IPP 4.1 may also extend to contracted service providers (**CSPs**).[11] When outsourcing to CSPs, organisations must ensure privacy and security obligations are reflected in contractual arrangements. Contracts should clearly define the roles and responsibilities of each party, including who 'owns', 'controls' or 'possesses' the information because this will affect who is accountable. Accountability for security cannot be outsourced.

4.39 A key part of governance measures which protect information security is how an organisation manages a security incident. Organisations should have a **security incident management process** in place to prepare for information security breaches and help them respond in a timely manner. A security incident management process could be supported by organisational training and awareness of security obligations.

4.40 One of the steps in a security incident management process is detection. Does your organisation have the capability to detect information security incidents? Detection capabilities can be integrated into the organisations systems and processes. For example, audit logs are discussed at paragraph [4.54].

4.41 When a data breach is detected, or the organisation is notified of a breach by an affected individual, the organisation should attempt to contain the breach and conduct a preliminary assessment. Evaluation of the privacy risks associated with the breach should take into account the type and sensitivity of the information that was compromised and the potential harm to individuals affected. Notification may be appropriate. However, if the harm caused by notification of an information

[9] OVIC, Victorian Protective Data Security Standard 1.
[10] Attorney-General's Department, *Protective Security Policy Framework*, Management structures and responsibilities: Foster a positive security culture (2016) p 15.
[11] Under a State contract which includes a clause that gives effect to s 17(2) of the PDP Act.

security breach is likely to be greater than the actual harm caused by the breach, notification to individuals might not be appropriate.[12] There may also be other security considerations in any data breach, and in this regard, organisations are encouraged to refer to Victorian Protective Data Security Standard 9, which involves reporting to OVIC.

4.42 Additionally, the organisation should implement steps to prevent the same type of incident reoccurring by conducting a post incident analysis of the causes of each incident and improve existing security measures. For more information, organisations can refer to OVIC's resource Managing the privacy impacts of a data breach.

Information security

4.43 Information security considers the protection of information throughout its entire lifecycle: from when information is collected, while it is held by the organisation and when it is disposed of. Organisations may need to take different steps to protect information at different times of its lifecycle. For example, when the form of the information changes from hard copy to soft copy, the information might become more accessible to others in the organisation and additional information security measures may be required to reasonably prevent misuse or unauthorised access.[13]

Case Study 4A: Governance of information security with regard to emails

Emails can contain or have attached, vast amounts of personal information. Care should be taken to get the email address right and not to send or forward copies to additional recipients who do not require the information.

To improve security of emails, organisations should establish what personal information can be sent via unencrypted email and whether alternative means of communication should be required for (certain types of) sensitive information.

4.44 A protective marking system can be a useful information security control. Protective markings indicate to anyone accessing the information the handling measures expected to be applied during the use, handling, storage, transfer and disposal of the information.

4.45 Where information sharing arrangements exist,[14] organisations should actively manage the agreements for relevance and currency. The agreement – for example, a memorandum of understanding – should address security from all security areas: governance, information, personnel, ICT and physical.

4.46 One part of information security is ensuring that access to information should be granted to the right

[12] See Office of the Victorian Privacy Commissioner, *Jenny's Case: report of an investigation into the Office of the Police Integrity pursuant to Part 6 of the Information Privacy At 2000,* (Report 01/06, 2006).
[13] Attorney-General's Department, *Protective Security Policy Framework*, Information security (2015).
[14] OVIC has published guidelines for sharing personal information in the Victorian public sector, including Family violence information sharing scheme and privacy law FAQs and Child information sharing scheme and privacy law FAQs.

people. Organisations may find the following considerations useful.

1. The amount or type of information accessible to certain employees should be appropriately limited according to their role. For example, does the individual's role in the organisation mean they should have 'read only' access or should they be authorised to change, add or delete information? How might this impact IPP 3 (Data Quality)?

2. Why might an individual need to access certain information assets? What uses might the information have? Will these uses be in line with IPP 2 (Use and Disclosure)? Might the individual be using the information for unauthorised or personal reasons?

3. If the information is accessible to contractors, or the organisation outsources functions or activities to CSPs, what level of access does the contractor require to do what they have been engaged to do? Those external to the organisations should not have any access to information not required by the service or function they have been contracted to provide.

4. Who might the information be disclosed to? Should the organisation specify who is an authorised recipient in the record of the information? Do, or should, information handling policies explain to employees who might be an authorised recipient? Or, alternatively, who is specifically *not* an authorised recipient?

Case Study 4B: Open access policy to student records results in security breach[15]

A soccer coach used his position as a teacher at the player's school to access her school records, which contained the student's medical information. The student's medical records were then used by the teacher and soccer club president to persuade the player and her parents to provide the soccer club with an indemnity in case she was injured during a game.

The school had no recorded policy or procedures to control access to students' records. The Department conceded it was in breach of the equivalent NSW Security Principle.

The NSW Administrative Decisions Tribunal commented that, in some cases, it may be appropriate for information to be widely available within a school to meet the purpose for which it was collected. However, in other cases, it may be more appropriate to limit the number of staff with access to a small group.

It was recommended that the school have guidelines for the use of personal information in student records and that staff be given appropriate training about their obligations under privacy legislation.

[15] *MT v Director General, NSW Department of Education and Training* [2004] NSWADT 194. This case was later appealed to the NSW Administrative Decisions Tribunal Appeal Panel, but the security breach was not the subject of the appeal.

Personnel security

4.47 Personnel security tries to make sure that only eligible and suitable people are engaged and employed and given access to information. This aspect of security is sometimes overlooked because organisations focus on data and not on the people who have access to it. Personnel security measures help organisations reduce the risk of information being compromised and contributes to creating a protective security culture where those who access information are aware of their security responsibilities.[16]

4.48 Pre-employment screening can be essential to ensure candidates and employees meet the organisation's security requirements. Ongoing personnel security management requires organisations to actively and consistently assess personnel risks. This includes risks associated with the changing suitability of employees for certain access and staff departures from the organisation.

ICT security

4.49 ICT security ensures information communication and technology systems that process and store information have adequate security measures. Digitisation of information assets means ICT security measures are critical to enable organisations to meet their business objectives while maintaining the security of personal information.

4.50 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.[17] For example, it might be reasonable and appropriate to encrypt sensitive information, as opposed to only protecting it with a password.

4.51 ICT security may be on-site or off-site. For example, organisations might use cloud solutions to host data that are located off-site, often outside Victoria. Data Security under IPP 4 and IPP 9 (Transborder Data Flows) are both particularly important in this circumstance.

4.52 Organisations should also consider Victorian Protective Data Security Standard 11 which states: 'An organisation establishes, implements and maintains Information Communications Technology (ICT) security controls.'

4.53 To help organisations prioritise ICT security controls to protect personal information, the Australian Cyber Security Centre (**ACSC**) has devised the 'Essential Eight' strategies.[18] They are:

> **Application whitelisting** of approved or trusted programs to prevent execution of unapproved or malicious programs including .exe, DLL, scripts and installers means. This means that all non-approved applications are prevented from executing malicious code.
>
> **Patch applications**, for example, Flash, web browsers, Microsoft Office, Java and PDF viewers patch or mitigate systems with 'critical' vulnerabilities within 48 hours. Organisations should use the latest versions of applications. This removes security

[16] Attorney-General's Department, *Protective Security Policy Framework*, 'Australian Government personnel security' (2016).
[17] Office of the Australian Information Commissioner, *Guide to securing personal information* (2018).
[18] Australian Cyber Security Centre, *Essential Eight Explained* (Webpage, April 2019).

vulnerabilities in applications which can be used to execute malicious code on systems.

Configure Microsoft Office macro settings to block macros from the Internet and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate. This prevents Microsoft Office macros from being used to deliver and execute malicious code on systems.

Use application hardening to configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Also, disable unneeded features in Microsoft Office (for example, OLE), web browsers and PDF viewers. This prevents malicious code being delivered and executed through these applications.

Restrict administrative privileges to operating systems and applications relevant to user duties. Organisations should regularly revalidate the need for privileges and separate these from normal access accounts (for example, not use privileged accounts for reading emails and web browsing). Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.

Patching operating systems (including network devices) with 'critical' vulnerability within 48 hours reduces the window of opportunity that intruders have to exploit a known vulnerability in an operating system.

Multi-factor authentication including for VPNs, RDP, SSH and other remote access for all users when they perform a privileged action or access in important or sensitive data repositories makes it harder for adversaries to access sensitive information.

Daily backups of important, new or changed data, software and configurations settings, stored in isolation from the production data and retained for at least three months ensures information can be accessed following a cyber security incident.

4.54 Audit logs can be a key ICT security tool. Audit logs allow organisations to see who has accessed what information if any misuse or unauthorised access or disclosure occurs. Audit logs can also deter security breaches because employees know their access of information systems will be tracked. To be an effective deterrent and detection measure, audit logs or audit trails must be usable and used. This means organisations need to be able to interpret the audit log and determine who accessed what information and when. An audit log may also reveal what was done with the information: if it was simply read, copied, forwarded, modified or deleted. The lack of capability to effectively audit and discover who had access to databases may amount to a breach of IPP 4.[19] An audit system that logs events – for example, access or changes to information – can ensure accountability of all user actions on a system. Audit and event logging can also improve the chances of an organisation detecting

[19] See, for example, Office of the Victorian Privacy Commissioner, *Mr C's Case: Report of an investigation pursuant to Part 6 of the Information Privacy Act 2000 into Victoria Police and Department of Justice in relation to the security of personal information in the Law Enforcement Assistance Program (LEAP) and E*Justice databases,* Report 03.06, July 2006.

malicious behaviour.[20]

4.55 Another ICT security measure which organisations might choose to implement as part of their 'reasonable steps' is the adoption of policies and procedures which govern how equipment which stores information is used. For example:

- **Laptop computers** can be stolen or lost, so safeguards should be considered to ensure that, if the equipment falls into the wrong hands, the information cannot be accessed. Encryption and password protection are obvious protections. Organisations might also provide staff with training about the types of information that should, or should, not leave the building.
- **USB Keys,** or memory sticks, can pose a serious security risk. Organisations might consider using encryption and adopting policies and procedures which advise staff about the following questions: Should USB keys be used? Under what conditions? Who is entitled to store what type of information on USBs?
- **End to end encryption** means data is encrypted when it is 'at rest' and in transit. Encryption of data in transit can protect sensitive or classified information when it is communicated over a public network infrastructure. Encryption does not reduce the sensitivity of information, but it mitigates the risk of harm if the information is compromised.[21]

Physical security

4.56 Physical security is about protecting places (for example, the office building) and objects (for example, mobile phones or laptop computers). Organisations must take steps to prevent unauthorised access to personal information as a result of poor physical security. To achieve this, organisations should ensure security measures designed to protect information are integrated into facilities, equipment and services.

4.57 To protect the physical security of personal information during the entire information lifecycle, organisations should establish, implement and maintain physical security measures which take into account the type of the information they hold, how the information is used and the potential harm to an individual should a security breach occur. Organisations need to provide a secure environment to protect hard copy (physical files) and soft copy (electronic documents) information. Organisations should implement multiple layers of security which might include:

- **Facilities:** designing specialist work spaces where sensitive information can be segmented to only permit access to those who have the appropriate authorisation and maintaining access logs to monitor staff movements within the physical environment.
- **Equipment***:* selecting security equipment to protect information during use or transfer, for example, satchels, tamper evidence bags, locked briefcases. Organisations should ensure secure containers are available for information to be locked away and support clear desk policies.
- **Services***:* monitoring and patrol of physical spaces, for example, with security guards or live monitoring of security camera feeds.

[20] For more information on event logging and auditing, organisations can refer to 'Guidelines for system monitoring' in the Australian Cyber Security Centre (**ACSC**)'s *Australian Government Information Security Manual*, (Report, May 2019) p 94.
[21] Australian Cyber Security Centre, *Australian Government Information Security Manual*, (Report, May 2019) 'Guidelines for using cryptography', p 123.

Case Study 4C: Improving physical security following a breach[22]

Medical documents, including patient prescriptions and pathology results were found scattered in a public park next to a private medical centre. The documents included patients names, addresses and telephone numbers. It was suggested the documents came from a large bin behind the private medical centre.

The Australian Privacy Commissioner considered reasonable steps to ensure data security depends on the circumstances in which personal information is held. Additionally, 'sensitivity of personal information stored is also an important factor and higher levels of scrutiny could be expected for more sensitive information, such as health information'.

An investigation found the bin had been tampered with and documents thrown around the park. The Commissioner and the medical centre devised a number of steps to improve data security, including secure fencing to reduce the risk of break in, locks, secure destruction of personal information (including shredding) and training for administrative and medical staff for proper destruction of personal information. The medical centre also wrote to all patients to advise them of the matter and the steps being taken to address it.

Distinguishing information security from information privacy

4.58 Privacy and security are intertwined concepts. An individual's information privacy cannot be ensured without proper security protecting personal information from being handled inappropriately. Information security is broader than information privacy because it is concerned with all official information, not just personal information, and is concerned with the confidentiality, integrity and availability of information. Security is about making sure the right people, at the right time have the right information.

Key terms used in IPP 4.1

Hold

4.59 Section 4 of the PDP Act provides an organisation 'holds' 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'.

4.60 This definition means an organisation can 'hold' information whether it has physical possession or not. The term 'hold' includes any record of personal information an organisation has control over. 'Holding' information in non-physical format is increasingly common with digital government.

4.61 In an outsourcing context, each organisation with control of personal information will have obligations under IPP 4.1. Organisations cannot contract out of the IPPs and obligations under the IPPs do not end if information leaves Victoria. This is because 'hold' depends on 'control' as well as 'possession'. An

[22] *Own Motion Investigation v Medical Centre* [2009] PrivCmrA 6.

organisation may not have 'possession' of information stored with a cloud service provider, however, if it retains 'control' of this information, IPP 4.1 will apply.

4.62 IPP 9 (Transborder Data Flows) may also be relevant to organisations using cloud storage outside Victoria because organisations in Victoria can 'hold' information stored outside of Victoria if they retain 'control' over it. The application of access and correction rights under IPP 6 also depends on what information the organisation 'holds'.

Misuse

4.63 'Misuse' of personal information occurs when it is used in a way that contravenes the IPPs or other restrictions around how personal information is used. Other restrictions include provisions in other legislation that require confidentiality or secrecy, or internal policies that prescribe appropriate uses of information. Misuse also includes using personal information for personal or financial gain.

4.64 Examples of a 'misuse' of personal information include:

- using someone's personal information to defraud or blackmail them. This is prohibited by the *Crimes Act 1958* (Vic).
- falsifying documents. For example, changing a friend's birth date in a record so they are entitled to a benefit they otherwise would not be.
- an employee of a local council using a database to get personal information about a resident's application for a house extension to help a friend oppose that extension application.
- exporting a mailing list from the organisation's database and using it for personal marketing.
- using contact information and other personal information to personally contact clients of the organisation with a view to profiting personally or harming a person's reputation.

Loss

4.65 Personal information is lost where its location is unknown. This can include both hard copy and electronic documents. Information that has been destroyed or de-identified is not lost.

4.66 Examples of a 'loss' of personal information include:

- Physical loss of a complainant's file while two government offices were moving offices. The file later arrived by post at the complainant's address, packaged with personal information about other persons and matters that did not concern the complainant.[23]
- Inability to locate digital files on the organisation's share drive when requested.
- A USB falling out of an employee's pocket on the street.
- Papers falling out of a folder while in transit from one place to another.
- Releasing information to another agency, without controls in place to limit that information's duplication or further use or disclosure by the other agency. It is unknown where the information might end up.
- Sending mail to the wrong address.
- Forgetting or leaving documents in a public place.

Unauthorised access, modification and disclosure

4.67 Accessing information involves viewing it in some form. Modification of information is changing the

[23] Office of the Victorian Privacy Commissioner, *Jenny's Case: report of an investigation into the Office of the Police Integrity pursuant to Part 6 of the Information Privacy At 2000,* (Report 01/06, 2006).

original information, or adding components to or removing components from the original information. Disclosing information involves making it accessible or visible to others. Access, modification or disclosure of information will be regarded as 'unauthorised' where a person:

- 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.

4.68 Examples of unauthorised access, modification and disclosure of personal information include:

- Using a colleague's login and password for a certain software program to access personal information not otherwise available to them.
- Changing someone's birth date in official records so they are eligible for a special entitlement. Falsifying documents can be misuse, as above, *and* unauthorised modification.
- Disclosing information provided in confidence about a colleague to another colleague.
- Taking a selfie in the office, with documents containing personal information in the background that is therefore disclosed to an employee's social circle.
- Verbal disclosure in a public place. For example, when employees discuss a person's personal information on public transport, others might easily hear. Verbal disclosures can be 'unauthorised disclosures' where the personal information also exists in recorded form.

Case Study 4D: Misuse and unauthorised access[24]

The complainant, a former employee of a government agency, complained her personal record had been accessed by a current employee of the agency who had used the records to locate the complainant's home. The complainant feared for her safety and, because of the incident, decided to change her name and relocate.

The agency's internal investigation showed the employee had had unauthorised access to the complainant's personal record. The Australian Privacy Commissioner found the 'inadequacy of the steps to prevent unauthorised access' meant the agency had not taken reasonable steps in the particular circumstances as required.

The matter was conciliated. The agency added additional protection to the complainant's personal information, terminated the employment of the individual responsible and the complainant accepted settlement of the costs for changing her name and residence.

IPP 4.2 Disposal of Data

4.69 IPP 4.2 requires organisations to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. While the Security Principle (IPP 4.1) aims to preserve and protect personal information from misuse, loss and unauthorised access, modification and disclosure, the Disposal Principle (IPP 4.2) aims to ensure organisations do not retain personal

[24] *F v Australian Government Agency* [2008] PrivCmr A 6.

information indefinitely where it is no longer required.

4.70 IPP 4.2 helps to minimise the potential security risks that arise when information is retained for too long. Disposal of information that is no longer needed reduces the possibility of the organisation inappropriately using out-dated information (see IPP 3 (Data Quality)). Additionally, disposing of information reduces the possibility of disparate data sets accumulated over time being aggregated for reasons unconnected to the original purpose of collection and beyond what the reasonable expectations might have been at that time. This would be an unauthorised use (see IPP 2.1) and an example of function creep. Disposal of out-dated and unnecessary information also removes the risk of inadvertent or unauthorised disclosure of that information.

4.71 Organisations can minimise the need to dispose of data by limiting the amount of identifiable information collected in the first place (IPP 1.1) and by providing opportunities for anonymous transactions (IPP 8).

4.72 Clear policies about retention and disposal of information help organisations comply with IPP 5 (Openness) which requires information handling policies to be made available on request. Organisations may choose to provide information about its retention and disposal policies at an early stage of collection, along with the other matters required to be in collection notices (IPP 1.3). Informing individuals about secure storage and intended disposal when organisations are collecting sensitive or delicate information can reassure individuals their information will not be later used for unrelated or unexpected purposes.

> **Case Study 4E: IPP 4.2 is incompatible with indefinite retention.[25]**
>
> An agency outsourced pre-employment screening to a company. The company's form used to collect information about potential employees stated all the information collected would be retained indefinitely by the pre-screening company. This information was to form part of the company's own database for the purpose of determining that person's suitability for any future positions.
>
> This was considered incompatible with the equivalent privacy principle by the New Zealand Privacy Commissioner. The company was instructed to destroy the information it held about the complainant.

Relevance of the Public Records Act

4.73 Most organisations bound by the PDP Act are also bound by the *Public Records Act 1973* (Vic) (**Public Records Act**). The Public Records Act prevails over the PDP Act to the extent of any inconsistency,[26] however, the record-keeping requirements under the Public Records Act and the disposal principle of IPP 4.2 can be read consistently with each other. Record-keeping obligations under the Public Records Act are a 'purpose' for organisation to retain the information. This means organisations are not

[25] *Case Note 218236* [2011] NZ Priv Cmr 4: Man objects to pre-employment screening.
[26] PDP Act, s 6.

required to destroy or de-identify any information they must retain under the Public Records Act.

4.74 Under the Public Records Act, public records cannot be destroyed unless authorised under the Public Records Office Victoria (**PROV**) Disposal Standard.[27] The Disposal Standard provides destruction can be 'authorised' through Normal Administrative Practice (**NAP**), Retention and Disposal Authorities (**RDAs**) or Single Instance Disposal Authorities (**SIDAs**).[28] If a relevant Records Authority from PROV (NAP, RDA or SIDA) does not apply to a particular record held by the organisation, the organisation should ask PROV to determine the appropriate disposal action.

4.75 Retention and Disposal Authorities (**RDAs**) are issued by PROV. They set mandatory minimum retention periods for records and authorised destruction of records once minimum retention periods have been met. Once the minimum retention period for a certain record has expired, the organisation is no longer required to keep that record. This means the organisation will need to reassess if they have another purpose for continuing to hold the information. If the record or information is no longer needed for any purpose, the organisation will need to take reasonable steps to destroy or de-identify the information under IPP 4.2. The potential for misuse or 'function creep' is reduced when the retention period is more strictly controlled.

4.76 Organisations are authorised to destroy certain records when doing so is part of their 'normal administrative practice' (**NAP**). Information that can be authorised to be destroyed using NAP include:

- Transitory messages, for example, calendars, personal emails
- Rough working papers, for example, rough meeting notes or notes preparing correspondence.
- Drafts not intended for further reference, in paper or electronic form
- Copies retained for reference purposes only
- Published material not included in the organisation's records.[29]

4.77 When an organisation has authority to destroy a public record, for example, according to a RDA or NAP, the organisation loses the purpose of retention for recordkeeping compliance with the Public Records Act. The organisation will need another legitimate purpose to keep the information or IPP 4.2 will require the organisations to take reasonable steps to destroy or de-identify the information.

'Reasonable steps to destroy or permanently de-identify'

4.78 Organisations can choose to destroy or de-identify personal information they no longer need. To meet the obligation of IPP 4.2, organisations need to be able to demonstrate they took reasonable steps to destroy or de-identify information. Reasonableness of destruction or de-identification will be assessed in the context of each particular case.

4.79 The sensitivity of information is an important factor that organisations should consider when thinking about what steps might be reasonable for IPP 4. If information falls within the definition of sensitive information in the PDP Act,[30] its handling, disposal or de-identification should be considered with particular care during risk assessment, when setting access controls and when assessing the timing and method of disposal.

4.80 Reasonableness involves considering how personal information is stored. The differences between various types of media that hold information, for example, hardware such as laptops or USBs and software such as information management systems or email, affect what amounts to reasonable steps

[27] Issued under s 12 of the Public Records Act.
[28] Public Records Office Victoria, *Disposal Standard PROS 10/13* (Standard, 2010).
[29] Public Records Office Victoria, *Disposal Standard PROS 10/13* (Standard, 2010) p 9.
[30] PDP Act, Sch 1.

for destruction or de-identification.

Destroying hard copy documents

4.81 When hard copy documents containing personal information are destroyed, this should be done securely. For example, they may be shredded by the organisation or a contractor. When contractors are used to dispose of information, organisations should remember accountability for security obligations cannot be outsourced. The contract agreement should include agreements to meet IPP 4 obligations. Case Study 4F demonstrates how unsecure disposal resulted in intact documents containing personal information being found as litter in a public park.

Destroying electronic documents

4.82 Destruction can be complex when data is held electronically. Actual and complete destruction may require the hardware itself be destroyed. Even when the primary version of an electronic document is destroyed, organisations may have back-ups of the information. 'Reasonable steps' to destroy information may not require all back-ups be destroyed where doing so is difficult or expensive. In such a case, a reasonable step to destroy the information may involve taking steps to limit access to back-ups of the information. Implementing technical, physical and organisations limits around access, use and disclosure, for example with access logs and audit trails, might mean the information is effectively 'beyond use'. This is a term used by the Office of the Australian Information Commissioner (**OAIC**) to reflect the difficulties of actually destroying personal information held in electronic format.[31]

4.83 The alternative to destruction is de-identification.

De-identification

4.84 'De-identified' is defined in s 3 of the PDP Act. De-identified information is 'personal information that no longer relates to an identifiable individual or an individual who can be reasonably identified'.

4.85 De-identification typically involves removing direct identifiers, for example, a name or address, and indirect or quasi-identifiers such as birth date or gender. It may also require additional steps to make it difficult to re-identify the information by linking it back to the person the information is about. For more information, see the Key Concepts section De-identification in practice.

4.86 De-identification is not a permanent state. De-identified information may be re-identified and reveal an individual's identity when other information is available that can be matched with the de-identified data.[32] If it is unclear what information may be matched, or the circumstances in which it may be matched, it is not possible to consider the information safe from re-identification. Organisations should consider periodically reviewing whether additional steps are required to maintain the data in sufficiently de-identified form.

'No longer needed for any purpose'

4.87 IPP 4.2 allows organisations to retain information for the purpose for which the information was collected, or for some other legitimate purpose authorised by IPP 2.1.[33] As discussed above at paragraph [4.73], meeting the record keeping obligations under the Public Records Act is a legitimate purpose. Other examples of legitimate purposes allowing information to be retained, other than for

[31] OAIC, *Chapter 11: APP 11 – Security of personal information* (March 2015).
[32] OVIC, *De-identification and privacy* (Background Paper, June 2018).
[33] *Caripis v Victoria Police* (Health and Privacy) [2012] VCAT 1472 (27 September 2012) [45]-[46].

the primary purpose of collection, include:

- if the information is necessary for research or statistics in the public interest, under IPP 2.1(c). For example, the Victorian Electoral Commission requires personal information to perform its statutory functions.
- if the information is necessary to lessen or prevent serious threats to health or safety of individuals or the public under IPP 2.1(d). For example, if an individual is dangerous, that danger might be kept on record to avoid future harm.

4.88 The purpose for retaining personal information should be specific and identifiable, rather than undefined and hypothetical. IPP 4.2 does not authorise retention of identifiable information 'just in case' it is needed for some future use by the organisation or by a third party. When organisations do not have one or more specific purposes for holding personal information, they must destroy or de-identify the information.

4.89 'Needed' has been interpreted as 'useful' or 'required'. The information does not need to be 'indispensable' to be 'needed' for another purpose.[34]

> Please send any queries or suggested changes to privacy@ovic.vic.gov.au. We will respond to privacy enquiries and consider your suggestions when we next update the Guidelines to the Information Privacy Principles.

Version control table

Version	Description	Date published
IPP 4 – Data Security 2019.B	Edits following consultation.	14 November 2019
IPP 4: Data Security 2019.A	Consultation draft.	1 August 2019
IPP 4: Data Security (2011)	2011 pdf version.	2011

[34] *Caripis v Victoria Police* (Health and Privacy) [2012] VCAT 1472 (27 September 2012) [44].