Guidelines for outsourcing in the Victorian public sector

Accompanying guide

Issued May 2017

Commissioner for Privacy and Data Protection

VICTORIA State Government

This page is intentionally left blank.

Guidelines for outsourcing in the Victorian public sector

Accompanying guide

Issued May 2017

Published by the Commissioner for Privacy and Data Protection
PO Box 24014
Melbourne Victoria 3001

First published May 2017

Also published on:
http://www.cpdp.vic.gov.au

ISBN 978-0-6480788-2-1

DOCUMENT DETAILS	
Security Classification	Public domain
Version	V.01
Issue Date	May 2017
Document Status	Final
Authority/Approval	Office of the Commissioner for Privacy and Data Protection (CPDP)

This page is intentionally left blank.

How to use this document

This guide serves as an accompaniment to the *Guidelines for outsourcing in the Victorian public sector – Checklist*, which aims to assist Victorian public sector bodies and their contracted service providers (CSPs) to effectively manage the privacy and data security of official information (public sector data and personal information) in outsourcing arrangements.

The checklist provides a high level overview of the matters that ought to be considered at each stage of an outsourcing arrangement, while this guide explores each question in more detail and explains the relevant requirements under the *Privacy and Data Protection Act 2014* (PDPA). The headings in this guide correspond with the question numbers in the checklist for ease of reference.

The documents are structured around three key phases of an outsourcing arrangement:

- *Planning the outsourcing arrangement*, covered by Steps 1-4
- *Implementing the outsourcing arrangement*, covered by Step 5
- *Concluding the outsourcing arrangement*, covered by Step 6.

Although the checklist and guide are primarily directed at Victorian public sector bodies, they provide a useful road map for CSPs to understand and prepare for the privacy and data security needs of their public sector clients.

The privacy requirements relate to *personal information* as defined under the PDPA; *health information* is expressly excluded from the remit of the checklist and guide. Outsourcing arrangements involving health information should be determined in accordance with the *Health Records Act 2001*.

The checklist and guide are intended to provide a starting point for the consideration of privacy and data security risks in an outsourcing arrangement. The matters canvassed here are of a general nature and **not exhaustive**. The documents may overlook risks and issues that arise in specific contexts, and organisations are encouraged to seek their own legal advice to ensure they are meeting their obligations.

These documents are guidelines only. They do not supersede information handling provisions in other legislation, and are not intended to create new policy for the Victorian public sector. Instead they describe the privacy and data security obligations that already exist under the PDPA, and aim to simplify the process for public sector bodies in navigating the regulatory landscape.

The checklist and guide assume a certain level of prior privacy and data security knowledge. Where possible, the guide refers to other materials that will provide further detail and explanation of key concepts.

Introduction

The PDPA establishes an information privacy and protective data security regime for the Victorian public sector. At the heart of the regime are two overlapping sets of obligations:

- When handling personal information, Part 3 of the PDPA requires public sector bodies to which that Part applies, to comply with the Information Privacy Principles (IPPs).[1]
- When handling public sector data, Part 4 of the PDPA requires public sector bodies to which that Part applies, to have regard to the Victorian Protective Data Security Framework (VPDSF), including the Victorian Protective Data Security Standards (VPDSS).[2]

Who is responsible for PDPA compliance in outsourcing arrangements?

In general, the PDPA applies to Victorian public sector bodies,[3] but not to the third party service providers that they may engage.[4] When a Victorian public sector body (the outsourcing party) enters into an outsourcing arrangement with a CSP, it is the outsourcing party that is primarily responsible for ensuring that those arrangements are consistent with both the VPDSF and the IPPs.

Under Part 4 of the PDPA, the outsourcing public sector body head is always held responsible for any data security breaches that may occur in relation to services provided under the outsourcing arrangement, even if those breaches are the result of the acts or practices of their CSPs.[5]

Under Part 3 of the PDPA, the default position is that the outsourcing party is liable for any privacy breaches that may occur in relation to services provided under the outsourcing arrangement, even if those breaches are the result of the acts or practices of their CSPs.[6] However, unlike under Part 4, this default position can be varied by State contract:

- If the outsourcing contract so provides, CSPs may be directly bound by the IPPs in the same way and to the same extent as the outsourcing party.
- Consequently, outsourcing parties may be excused from liability for a breach of the IPPs that are the result of the acts or practices of a CSP, if:
  - the CSP has assumed liability for its own actions under the PDPA; and
  - the PDPA is capable of being enforced against the CSP.[7]

Note

This mechanism does not excuse outsourcing parties from liability for their own actions in relation to the outsourcing arrangement.

1 See *Privacy and Data Protection Act 2014*, Part 3.

2 See *Privacy and Data Protection Act 2014*, Part 4. The VPDSF was published in June 2016 and comprises 18 Victorian Protective Data Security Standards (VPDSS), an Assurance Model, and supporting security resources. The VPDSF is available online at https://www.cpdp.vic.gov.au/menu-data-security/victorian-protective-data-security-framework/vpdsf.

3 See *Privacy and Data Protection Act 2014*, s 13 for the organisations to which Part 3 applies and s 84 for the bodies to which Part 4 applies.

4 Unless the outsourcing contract provides that they are to be bound by the IPPs, in which case the service provider becomes an organisation to which Part 3 of the PDPA applies. See *Privacy and Data Protection Act 2014*, ss 13(1)(j and 17(2), discussed below. There is no similar mechanism for Part 4 of the PDPA.

5 *Privacy and Data Protection Act 2014*, s 88.

6 *Privacy and Data Protection Act 2014*, s 17.

7 *Privacy and Data Protection Act 2014*, s 17(4).

If a CSP chooses to subcontract some of its functions or activities under the State contract, a subcontractor may also have obligations under Part 3 of the PDPA. If a CSP has assumed responsibility for privacy obligations by way of State contract, they can then pass these obligations on to the subcontractor. If, however, the CSP did not assume the outsourcing party's responsibilities, the original outsourcing party will remain liable for the acts or practices of the subcontractor. The original outsourcing public sector body head will always retain liability for data security under Part 4 of the PDPA.

Other tools and guidance

When planning and implementing outsourcing arrangements, outsourcing parties should be mindful of the *Victorian Government Risk Management Framework*, which requires organisations to identify, assess and manage all risks to which they are exposed, including risks associated with the handling of official information.[8]

Outsourcing parties should conduct a **Security Risk Assessment** (SRA)[9] and where necessary, incorporate protective data security measures into the outsourcing contract if the CSP will:

- have **direct access** to official information (for example, if access to official information is required for the performance of the contracted service), or
- have **indirect access** to official information (for example, if the CSP may incidentally come into contact with official information), or
- **generate (collect, capture, record)** information on behalf of the outsourcing party (for example, if the CSP is to collect data and/or produce a report as part of the contracted services).

Outsourcing parties should also conduct a **Privacy Impact Assessment** (PIA)[10] and where necessary, incorporate privacy-protective measures into the outsourcing contract if the outsourcing arrangement involves:

- handling any personal information, including the collection, holding, management, use, disclosure or transfer of personal information, or
- changes to personal information handling practices.

8 Department of Treasury and Finance, *Victorian Government Risk Management Framework*, March 2015.

9 Further information on Security Risk Assessments can be found in the VPDSF, available online at: https://www.cpdp.vic.gov.au/menu-data-security/victorian-protective-data-security-framework/vpdsf.

10 Further information on Privacy Impact Assessments can be found online at: https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-checklists-and-tools.

Tip for CSPs

Remember that any failure to comply with the VPDSF or the IPPs in the performance of functions under a State contract will expose either the CSP itself or its public sector clients to liability under the PDPA; whatever the outsourcing arrangement, it is essential for all CSPs to consider the VPDSF and the IPPs when handling official information.

Privacy and data security protections are most effective when they are embedded into the culture and processes of an organisation, rather than bolted on as an afterthought to a project or activity. This may require changes to organisational culture, business processes, or physical and ICT infrastructure. Because of this, CSPs should be proactive in understanding the VPDSF and IPP requirements that are likely to accompany the work they do for Victorian public sector bodies, and might consider investing in the infrastructure, policies and practices that will enable them to meet those requirements. Not only does a proactive approach lead to cheaper and more effective compliance, it is also likely to provide a competitive advantage, as public sector bodies are likely to prefer CSPs that can demonstrate maturity in handling official information in accordance with the PDPA.

CSPs should conduct their own SRA and PIA, and where necessary, adopt appropriate privacy and protective data security measures.

Step One — Planning the outsourcing arrangement

1.1 Consider privacy and data security in the design of the outsourcing arrangement

Before taking steps to commence an outsourcing arrangement, outsourcing parties should carefully consider the potential costs and benefits associated with the proposed arrangement, including the costs associated with managing information-related risks and ensuring VPDSF and IPP compliance.

Where possible, outsourcing arrangements should be structured to minimise the number of people and organisations that have access to official information (particularly if it includes personal information). This can help to minimise information-related risks and compliance costs for outsourcing parties and for CSPs.

CSPs' access to official information should be on a 'need to know' basis. When planning an outsourcing arrangement, consideration should be given to exactly what information will be required by a CSP to provide the contracted services efficiently, and what mechanisms are available to restrict CSP access to only that information.

In some cases, where an activity requires access to large amounts of personal or significant information and the benefits of outsourcing are marginal, retaining the function in-house may present better value for money, and greater privacy and data security protections.

For example, the assessment of eligibility for a government service may require access to a large amount of personal information, whereas the actual provision of the service may not. An outsourcing party may wish to retain eligibility assessments as an internal function, in order to minimise the amount of information that needs to be accessed by the CSP.

Tip for CSPs

You can add value by working with the outsourcing party to design an outsourcing arrangement that minimises risks to official information. For example, by finding new ways for the CSP to provide a particular service efficiently without having access to large amounts of personal information about the recipients. This could happen up front, in the original design of the outsourcing arrangement, or during the course of the engagement.

1.2 Identify and assess the value of all information that may be affected by the outsourcing arrangement

Identify affected information

Outsourcing parties should carefully consider what information may be accessed, generated or affected by a proposed outsourcing arrangement. This includes:

- Information to which the CSP will have **direct access** (for example, information that is required by the CSP for the performance of the contracted service).
- Information to which the CSP may have **indirect access** (for example, information that may be incidentally accessible to a CSP while cleaning the outsourcing party's offices, or incidentally available to ICT contractors employed to manage or repair the outsourcing party's ICT systems).
- Information which the CSP will **generate** on behalf of the outsourcing party (for example, information collected from users of an outsourced service).
- Information whose confidentiality, integrity or availability may be **affected** by the contracted services, whether or not the CSP has access to it (for example, a telecommunications service provider may not have access to official information, but the contracted services may be essential to the continued availability of that data).

Assess the value of affected information

Outsourcing parties should adopt a risk-based approach to protecting official information. This means that the level of assurance that should be sought and the extent to which controls should be implemented depends on the kinds of information that are involved. The greater the consequences of a compromise to the confidentiality, integrity or availability of the information, the greater the effort expected from organisations to guard against that risk.

For example:

- If the affected information is **publicly available**, then only the integrity and availability of the information will need to be managed.
- If the affected information is **UNCLASSIFIED**,[11] requires a **Dissemination Limiting Marker** (DLM)[12] or has a **Business Impact Level** (BIL)[13] of 1, then specific controls may need to be included in contract arrangements to protect the information (based on the outsourcing party's risk assessment and internal information management procedures).

11 UNCLASSIFIED is not recognised as a protective marking and is not to be applied to security classified information. Compromise of UNCLASSIFIED information could be expected to cause insignificant harm/damage to government operations, organisations or individuals. For further information see the VPDSF at: https://www.cpdp.vic.gov.au/menu-resources/resources-data-security/vpdsf-resources.

12 Dissemination Limiting Markers (DLMs) are markings for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling. For further information see the VPDSF at: https://www.cpdp.vic.gov.au/menu-resources/resources-data-security/vpdsf-resources.

13 Information has a Business Impact Level (BIL) of 1 when compromise could be expected to cause limited harm/damage to government operations, organisations and individuals. For further information see the VPDSF at: https://www.cpdp.vic.gov.au/menu-resources/resources-data-security/vpdsf-resources.

- If the affected information requires a security classification of **PROTECTED**[14] or above or has a **BIL** of 2[15] or above, then additional, specific controls may need to be included in the contract arrangements to strictly limit access to the information to CSP personnel with the relevant security clearance and a need-to-know, and to prevent unauthorised access to the information from within or outside the CSP. Controls should be at least equal to those required within the outsourcing party.
- If the information is (or contains) **personal information**, then further controls may need to be implemented in order to comply with the IPPs (in addition to any controls applied on the basis of the BIL of the information).

Tip for CSPs

Consider the nature and value of official information that is typically involved in the work you do or intend to do for public sector clients, and be ready to provide or implement the necessary controls.

1.3 Be aware of any relevant secrecy or information handling obligations

Outsourcing parties should consider whether access to, or use of, information affected by the outsourcing arrangement is subject to information handling provisions in other legislation, including enabling legislation. If so, steps should be taken to ensure that the outsourcing arrangement is consistent with these requirements.

If the proposed outsourcing arrangement does not comply with secrecy and information handling provisions in other legislation, outsourcing parties may need to reconsider its design. In some cases, where the arrangement is in the public interest and its objectives cannot be achieved in any other way, it may be appropriate to seek an Information Usage Arrangement (IUA) from the Commissioner for Privacy and Data Protection (CPDP). A IUA is an arrangement whereby certain acts or practices are deemed 'authorised or required by law' for the purposes of an information handling provision. Following the Commissioner's approval, an IUA requires the approval of the relevant Ministers.[16]

Outsourcing parties should also review their privacy policies and collection notices to ensure that the proposed outsourcing arrangement is consistent with the information they are communicating to the public. In some cases, outsourcing parties may need to update their privacy policies to reflect the new information flows, and notify affected individuals if the outsourcing arrangement involves new uses or disclosures of personal information that were not contemplated at the time of collection.

14 PROTECTED is a security classification for information whose compromise to its confidentiality could be expected to cause major harm/damage to government operations, organisations or individuals. For further information see the VPDSF at: https://www.cpdp.vic.gov.au/menu-resources/resources-data-security/vpdsf-resources.

15 Information has a BIL of 2 when compromise could be expected to cause major harm/damage to government operations, organisations and individuals. For further information see the VPDSF at: https://www.cpdp.vic.gov.au/menu-resources/resources-data-security/vpdsf-resources.

16 More information about IUAs can be found on the CPDP website: https://www.cpdp.vic.gov.au/menu-privacy/privacy-laws-and-standards/privacy-laws-and-standards-flexibility-mechanisms.

Step Two — Choosing the right CSP

Before engaging a CSP, outsourcing parties should conduct an appropriate level of due diligence to be satisfied that the CSP will be able to comply with all contractual and statutory requirements pertaining to privacy and data security, and manage any information-related risks that may arise.

For low risk outsourcing arrangements, this may amount to a cursory check that the CSP is actually capable of delivering what is required. For more complex, high value, long term or high-risk arrangements, due diligence may include a detailed assessment of the organisation's financial stability, legal risks, technical capacity and infrastructure.

In general, the CSP should be a mature, reliable and reputable organisation capable of handling and dealing with official information in accordance with the PDPA. It should have effective security governance arrangements in place and consistently apply risk-managed security practices across the four security domains (information, personnel, ICT and physical security). If the CSP will be handling personal information, it should also have mechanisms in place to ensure the collection, holding, management, use, disclosure, transfer, and access to personal information occurs in compliance with the IPPs.

Tip for CSPs

Consider the criteria that outsourcing parties will be looking for when selecting a CSP. Be proactive in understanding the VPDSF and IPP requirements that are likely to accompany the work that you wish to do for Victorian public sector bodies. Investing in advance in the infrastructure, policies and practices that will enable you to meet those requirements will provide a competitive advantage when bidding for public sector work.

Failure to properly assess a CSP prior to engagement could be considered a failure by the outsourcing party to meet the requirements of VPDSS 9 (which requires outsourcing parties to ensure that the outsourced service complies with the VPDSS), and if personal information is involved, IPP 4 (which requires organisations to take reasonable steps to ensure adequate data security).

At a minimum, an outsourcing party should consider:

1. Whether the CSP is sufficiently resourced to provide adequate privacy and data security protections.
2. The privacy and data security culture and track record of the CSP.
3. Whether the CSP will engage a subcontractor (or subcontractors).
4. Whether the CSP is an interstate or overseas organisation, and whether information will be transmitted or stored outside of Victoria.

2.1 Consider whether the CSP is sufficiently resourced to provide adequate privacy and data security protections

Outsourcing parties should ensure that a CSP is sufficiently resourced to comply with the PDPA. The costs (both financial and reputational) of a data breach by a CSP will usually be higher than the costs of taking preventative measures, particularly if the breach involves personal information.

There may be costs for a CSP to comply with the VPDSF and the IPPs. Depending on the CSP and the nature of the engagement, this may require developing improved security governance practices, personnel screening, and physical and ICT security upgrades. It may also include installation of new or updated document management systems and/or electronic databases to capture, transmit, carry and securely store information.

If the CSP is not sufficiently resourced to provide adequate privacy and data security protections, an outsourcing party may wish to:

- commit some of their resources to getting the CSP up to the required standard (for example, by funding security upgrades, providing equipment and expertise, or arranging for work to be carried out on the outsourcing party's secure premises)
- redesign the arrangement to lower the security requirements for the CSP (for example, by limiting their access to high value information, or retaining certain activities in-house)
- consider other providers who are better able to meet their needs.

Tip for CSPs

Consider the costs of VPDSF and IPP compliance when bidding for Victorian public sector work, and be open about the your current security posture and any work that might need to be done to meet the required standards. In most cases, outsourcing parties will be able to assist you. It is better to plan for these matters up front than to realise part way through a contract that significant investment is needed in order to ensure compliance.

2.2 Consider the privacy and data security culture and track record of the CSP

An outsourcing party should ensure that the CSP has demonstrated a commitment and willingness to meet its privacy and data security obligations and that it has, or will, provide staff members who handle official information with appropriate training, screening, and if necessary, security clearances. Service providers should easily be able to articulate the steps they take to ensure privacy and data security.

Care should be taken when dealing with CSPs with a history of data breaches or similar incidents, unless they are able to demonstrate that they responded quickly and effectively, and that the root causes of the incidents have been remediated.

If the CSP is unable to demonstrate their privacy and data security practices, outsourcing parties may wish to consider, as above:

- committing some of their resources to getting the CSP up to the required standard (for example, by funding security upgrades, providing equipment and expertise, or arranging for work to be carried out on the outsourcing party's secure premises)
- redesigning the arrangement to minimise the impact of a failure by the CSP to meet its privacy and security obligations (for example, by limiting their access to high value information, or retaining certain activities in-house), or
- engaging another provider with a better track record.

Where an outsourcing party has entered into an arrangement with a CSP who is unable to adequately demonstrate their privacy and data security practices, the risks of this arrangement need to be documented, accepted and managed throughout the lifecycle of the contract.

2.3 Consider whether the CSP will engage a subcontractor (or subcontractors)

Outsourcing parties should confirm the extent to which the CSP will engage subcontractors to perform functions or activities the CSP has been engaged to perform. If the CSP intends to use a subcontractor to perform some of the functions or activities, that secondary outsourcing relationship (between the CSP and their subcontractor) should be subject to the same level of scrutiny as the primary relationship (between the outsourcing party and the CSP).

If the CSP will engage subcontractors, the outsourcing party should confirm with them the nature of the subcontracted work and the potential privacy and data security risks it may pose. The outsourcing party should ensure that appropriate steps are being taken to manage any privacy and data security risks that may arise from the subcontracting arrangement (for example, by reviewing the CPDP checklist and addressing any risks that may be identified).

Tip for CSPs

Consider the VPDSF and the IPPs when engaging subcontractors that you might rely on to perform services under a State contract, and consider which party will assume liability for a breach. It is important that subcontractors understand and agree to comply with any IPP or VPDSF requirements in relation to Victorian public sector work.

2.4 Consider whether the CSP is an interstate or overseas organisation, and whether information will be transmitted or stored outside Victoria

There are additional risks associated with storing or processing information in another jurisdiction, whether interstate or overseas. For example, like Australia, most foreign jurisdictions have legislative powers that allow access to communications and stored information for the purposes of law enforcement and national security. Even when data is held locally, foreign-owned companies doing business in Victoria may be subject to foreign legislative requirements that may compromise the confidentiality, integrity or availability of official information.

Other risks associated with storing information offshore include complications arising from information being simultaneously subject to multiple legal jurisdictions, the lack of transparency (and reduced ability to directly monitor operations), greater risk to the security of data in transit, and the difference in the business and legal cultures in other jurisdictions.

Victorian public sector bodies have obligations under IPP 9, which limits the transborder flows of personal information to certain circumstances. Outsourcing parties should ensure they are compliant with these restrictions if choosing to engage a CSP located outside Victoria. Guidance on IPP 9 and transborder data flows can be found in the *Guidelines to the Information Privacy Principles*.[17]

17 These guidelines are based on the *Information Privacy Act 2000*, which was replaced by the PDPA with the establishment of the Office of the Commissioner for Privacy and Data Protection in September 2014. The IPPs were incorporated into the PDPA without amendment. The guidelines are available online, at: https://www.cpdp.vic.gov.au/images/content/pdf/privacy_guidelines/OVPC%20Guidelines%20to%20the%20IPPs%20Edition%203%202011.pdf/.

If official information will be transferred outside Victoria, outsourcing parties should consider, document, accept and manage any risks to privacy, data confidentiality, integrity or availability that may arise from another jurisdiction's legislative requirements. If the CSP is based outside Victoria, the PDPA may not be enforceable against the CSP. This means that the outsourcing party will always be responsible for any acts or practices of the CSP that may breach the IPPs (that is, outsourcing parties will not be able to rely on section 17 of the PDPA to allocate responsibility to their CSP for IPP compliance under the State contract).[18] This should be taken into consideration when choosing the right CSP.

CPDP has produced a discussion paper on *Cloud computing in the Victorian public sector*, which may assist outsourcing parties considering using cloud services.[19] Further guidance on cloud computing can also be found in the *Australian Government information security management guidelines – Risk management of outsourced ICT arrangements (including Cloud)*[20] and the *Australian Government Cloud Computing Policy*.[21]

Tip for CSPs

If you are based outside of Victoria, you may need to provide additional assurances that the privacy, confidentiality, integrity and availability of information can be maintained. You may wish to consider structuring your offerings in ways that include security measures, minimise the amount of official information that you have access to and/or ensure that official information remains within Victoria.

18 This is because section 17 of the PDPA provides that outsourcing parties may only avoid liability for the CSP's actions if the CSP has assumed direct liability (via a provision in the State contract) and the PDPA is enforceable against the CSP.

19 See https://www.cpdp.vic.gov.au/images/content/pdf/Cloud_Computing_in_the_Victorian_Public_sector.pdf.

20 See https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentInformationSecurityManagementGuidelines.pdf.

21 See http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf.

Step Three — VPDSF planning and due diligence

Under the VPDSF, the public sector body head of an outsourcing party is always held responsible for any breaches that may occur in relation to services provided under an outsourcing agreement, even if those breaches are the result of the acts or omissions of the CSP.

In general, an outsourcing party needs to make sure that a CSP implements security controls in relation to the official information they collect, hold, manage, use, disclose or transfer, that are at least equal to those in place within the outsourcing party. Security controls may relate to governance, information security, personnel security, ICT security and physical security.

3.1 Governance — Roles and responsibilities

If official information will be available to CSP personnel outside of the outsourcing party's facilities, the outsourcing arrangement should stipulate the responsibilities and accountabilities of each party so all roles and responsibilities are clearly understood. The arrangement should also identify the key security point(s) of contact in the CSP who are responsible for protective data security, and require the CSP to advise of all their personnel (including subcontractors) who will have access to official information. The outsourcing party should be kept informed of any access changes throughout the life of the arrangement.

If the CSP will only access official information within the outsourcing party's facilities, the outsourcing party should identify a point of contact for the proposed CSP. The outsourcing party's responsible officer for personnel security should require pre-acceptance of proposed CSP personnel who will have access to the outsourcing party's facilities or information.

Tip for CSPs

Be prepared to be flexible about where and how the contracted services will be performed. Depending on the information involved, some outsourcing parties may require that all work be done in their facilities and/or on their systems.

3.2 Governance — Training and awareness

Outsourcing parties should consider whether there is a need for CSP personnel to complete initial and/or ongoing protective data security training and awareness programs, above that which may already be provided by the CSP.

If the information provided to or generated by the CSP will require a security classification of PROTECTED or above, or have a BIL of 2 or above, the outsourcing party should require CSP personnel to complete initial and ongoing protective data security training and awareness requirements at least equal to those required within the outsourcing party. This may cover:

- measures to limit access and prevent unauthorised disclosures
- procedures for reporting actual or suspected security incidents, and
- protocols governing which CSP personnel are authorised to access the outsourcing party's security classified information.

3.3 Governance — Incident management and reporting

There is always potential for a security breach to occur, irrespective of how robust the security measures implemented may have been. Outsourcing parties should prepare for the likelihood of a breach, by:

- specifying agreed incident management processes as part of outsourcing arrangements, including roles and responsibilities of the outsourcing party and the CSP, notification and response timeframes, who leads an investigation, and reporting requirements
- requiring the CSP to report any incident involving the outsourcing party's information within specified timeframes – this includes unauthorised access, disclosure, modification or unavailability of the information
- making provision for free and full access to the CSP's facilities and systems for the purposes of investigating data security breaches; and
- detailing any actions that may be taken as a result of serious data security breaches, noting the importance of frank and timely reporting of incidents by the CSP. The outsourcing party should work with the CSP to mitigate any incidents and prevent re-occurrences. Only when there is an inability or unwillingness to address incidents, or a failure to report them, should punitive action be taken against the CSP.

Outsourcing parties should also consider whether other security incidents, not directly related to the contracted services, should be reported (for example, breaches of the CSP's or other clients' information). These can give an overall picture of the security status of the CSP.

Tip for CSPs

Security breaches happen. In most cases, it is the way that the CSP handles the breach, rather than the fact that the breach occurred, that has the biggest impact on the outsourcing party's trust and confidence going forward. Promptly reporting breaches and working closely with the outsourcing party to mitigate any consequences and prevent re-occurrences is likely to lead to a stronger client relationship.

3.4 Governance — Business continuity

If there is a requirement for certain information affected by the outsourcing arrangement to be available within specific timeframes, or if there are negative impacts that could arise from loss of certain information affected by the outsourcing arrangement, then the outsourcing party should consider establishing or specifying business continuity measures. These may include:

- information backup requirements
- unavailability notification requirements
- maximum and preferred time the information can be unavailable
- disaster recovery procedures.

3.5 Governance — Compliance and oversight

If the outsourcing arrangement is to be ongoing or in place for an extended period, the outsourcing party should consider instigating procedures for periodic compliance checks. These may include spot checks of implemented security measures (such as audit logs), process reviews or facility inspections. These checks could be undertaken by the outsourcing party or an agreed-upon independent party.

If the arrangement is long-term, outsourcing parties should also require annual attestations of compliance with any security requirements identified as part of the outsourcing arrangement.

3.6 Governance — Transfer of data back to outsourcing party on termination or completion of contract

If official information that is not publicly available will be provided to or generated by the CSP, the outsourcing arrangement should provide for the return or disposal of that information upon completion or termination of the arrangement.[22]

Unless there are specific destruction provisions in place, all copies of information should be returned to the outsourcing party at the conclusion of the contract. It may not be possible to fully remove the outsourcing party's information from the CSP's ICT system, however sanitisation should be undertaken to the extent possible.

The outsourcing party should also include provisions in the State contract to:

- require attestation by the CSP at the conclusion of the contract that all of the outsourcing party's information has been disposed of or returned
- require the return or decommissioning of any security measures provided by the outsourcing party
- allow audit of the CSP systems/facilities to ensure information has been removed.

Tip for CSPs

Where possible, official information should be segregated from any other information held by the CSP (see 3.10 below). If official information is only kept on specific hardware, or on specific systems, the return or disposal of information at the conclusion of the contract will be a much simpler process.

3.7 Information security — Protective markings and hardcopy documents

Outsourcing parties should require CSPs to respect and observe protective markings that have been applied to official information, and to apply the relevant protective markings to new information where appropriate.

Outsourcing parties should also specify any required security measures for hardcopy information throughout its lifecycle, including creation, receipt, access and disclosure, copying and scanning, storage, auditing, use, removal, transfer and disposal. These controls should not be lower than the outsourcing party's internal measures for similar hardcopy information.

22 In accordance with Public Records Office Victoria Recordkeeping Standard *PROS 10/13 Disposal*.

3.8 Personnel security — Employment screening

Outsourcing parties should require initial and ongoing screening of all CSP personnel with access to official information, based on the outsourcing party's risk assessment and internal information management procedures. This screening should at least meet *Australian Standard 4811 — Employment Screening*.[23]

If the information provided to or generated by the CSP will require a security classification of PROTECTED or above, or have a BIL of 2 or above, the outsourcing party should require the CSP to:

- obtain appropriate security clearances for all CSP personnel with potential access to any security classified information, including any person with out-of-hours or unescorted access to the facility where the information is held (such as cleaners); and
- proactively advise the outsourcing party of any concerns with CSP personnel that have potential access to the outsourcing party's information.

Additionally, outsourcing parties should require CSPs to provide and maintain a list of all CSP personnel, including subcontractors that have access to official information as part of the outsourcing arrangement. Where appropriate, personnel with access to official information should complete deeds or undertakings as to confidentiality.

If the CSP does not have pre-employment and ongoing screening processes for *all* its personnel, the outsourcing party should consider the extent to which this may be a risk. For example, what is the risk associated with incidental or unauthorised access to information by unscreened personnel?

Tip for CSPs

It is important that CSPs understand any personnel screening requirements well in advance of beginning work, and that they are in a position to provide personnel who meet those requirements. Some security clearances can take months to obtain.

Additionally, some CSP personnel who do not have authorised access to official information may nevertheless require some level of clearance to address risks associated with incidental and unauthorised access.

Additionally, some CSP personnel who do not have authorised access to official information may nevertheless require some level of clearance to address risks associated with incidental and unauthorised access.

23 See https://www.saiglobal.com/pdftemp/previews/osh/as/as4000/4800/4811-2006.pdf.

3.9 ICT security

The CSP's ICT systems should meet or exceed the controls used by the outsourcing party. The *Australian Government Information Security Manual* contains relevant requirements for electronic information during the information lifecycle.[24]

Data transfers

If official information will be collected by or provided to the CSP electronically, the outsourcing party should ensure that measures are in place to manage the security of the information while in transit. Appropriate standards of encryption should be used if data is transferred over the internet or on an internet facing system.

Storage

If official information will be stored and/or accessed electronically, outsourcing parties should ensure that CSPs appropriately manage access to any of their systems that contain official information.

For example:

- The CSP's ICT systems controls should restrict access to the areas of their systems holding the outsourcing party's information to only the CSP's personnel with a need-to-know.
- Ideally the outsourcing party's information should be stored separately from any other information held by the CSP. This could be on separate servers or within a compartment of the CSP's system.

Disposal

If electronic data will be disposed of by the CSP, rather than returned to the outsourcing party when no longer required, the outsourcing party will need to ensure that the CSP understands and follows any information disposal requirements, including any record keeping requirements, that must be met. For example, there may be specific requirements and standards for erasure of information from hard drives or destruction of portable digital media, particularly in relation to security classified information. All copies provided to/made by the CSP should be accounted for and destroyed at the time of the original information disposal.

The outsourcing party should identify any limitations to the full removal of electronic information from CSP systems prior to providing them with official information.

The outsourcing party should also stipulate any specific requirements for disposal during the upgrading or maintenance of a CSP's faulty or outdated ICT systems. For example, old hard drives that contain official information should be returned to the outsourcing party or sanitised before they are discarded.

An outsourcing party should also consider its obligations under the *Public Records Act 1973* (PRA) for storage and disposal of public records, and should confirm with the Public Record Office of Victoria (PROV) if a proposed storage or disposal plan complies with the PRA.

24 See https://www.asd.gov.au/infosec/ism/.

Tip for CSPs

Returning and deleting information is not always a straightforward process. For example, there may be technical barriers to fully removing the outsourcing party's data from your systems. Planning ahead and isolating information related to the outsourcing arrangement on specific hardware or with specific people, can make the process significantly more efficient.

As discussed at 3.6 above, isolating official information on specific systems and hardware will streamline the disposal process. CSPs that are able to provide assurances as to how and where official information will be stored, and the processes by which it will be disposed of, are likely to be preferred.

CSPs who are asked to destroy documents should also consider whether they have any obligations under the PRA for storage and disposal of public records. CSPs should confirm with PROV whether a proposed storage or disposal plan complies with the PRA.

3.10 Physical security

Outsourcing parties should review a CSPs' physical security measures and require that they meet or exceed their own internal requirements for similar information. For example:

- The requirement for electronic access control systems and security alarm systems should be determined based on at least the outsourcing party's own requirements for information at the same BIL.
- Access to CSP facilities should be controlled, with all physical access to the outsourcing party's hard copy information or hardware storing the outsourcing party's electronic information limited to CSP personnel with a need to access the information.
- Public access to the CSP's facilities containing the outsourcing party's information should be restricted, with only approved and escorted visitors allowed access.
- Based on a risk assessment of the CSP's facilities, outsourcing parties may require the CSP to store any hardcopy and portable electronic devices holding the outsourcing party's information, within a storage container at least equivalent to those used by the outsourcing party for similar information.
- System hardware holding the outsourcing party's electronic information should be in an approved secure storage rack suitable for information of that BIL.
- CSPs should advise the outsourcing party of any incidents or concerns with the physical security of the CSP facilities used to store or process the outsourcing party's information as they arise.

If the information provided to or generated by the CSP will require a security classification of PROTECTED or above, or have a BIL of 2 or above, the outsourcing party should consider additional, specific controls, including:

- The type and capability of security alarm systems to protect areas holding the outsourcing party's information.
- Secure storage requirements for hardcopy and electronic devices containing the outsourcing party's information.
- Physical security of ICT systems. For more details, refer to the *Australian Government Information Security Manual*[25] and the *Australian Government physical security management guidelines – Physical Security of ICT equipment, systems and facilities*.[26]

25 See https://www.asd.gov.au/infosec/ism/.

26 See https://www.protectivesecurity.gov.au/physicalsecurity/Pages/PhysicalSecurityOfICTEquipmentSystemsAndFacilitiesGuidelines.aspx.

Step Four — IPP planning and due diligence

**** Step 4 only applies to outsourcing arrangements that involve personal information.***

4.1 Liability for compliance with the IPPs

If the CSP has assumed direct liability for their compliance with the IPPs, then they themselves will be liable for any breaches of the IPPs. This is a strong incentive for CSPs to comply. However, not all CSPs will be familiar with the requirements of the PDPA or have policies and procedures in place that are sufficient to ensure compliance. For example, a small organisation that does not ordinarily provide services to government may have never been subject to Commonwealth or State privacy laws before, and may not even have a privacy policy.

As noted above, where a CSP has assumed direct liability for compliance with the IPPs and where the PDPA is capable of being enforced against them, outsourcing parties may avoid liability for any acts or practices of the CSP that may breach the IPPs. However, outsourcing parties remain responsible for their own acts and practices surrounding the outsourcing arrangement, including their decisions to engage a specific provider, or to enter into, maintain or terminate a particular arrangement.

For example, an outsourcing party may breach IPP 4 by entering into an outsourcing arrangement whereby a small not-for-profit organisation with limited experience in information security is trusted with large amounts of sensitive personal information (even though liability for a specific breach may rest with the CSP).

Similarly, private sector CSPs may have less experience with the concept of the right to access and correct personal information, compared with Victorian public sector bodies. Rights to access and correct government-held personal information in Victoria have existed since 1982 under the *Freedom of Information Act 1982*, however the right to access and correct personal information is a relatively recent phenomenon for private sector organisations.[27] As a result, it may not be reasonable to simply assume that even a large and well-resourced private sector CSP will implement appropriate processes to comply with IPP 6.

As a result, even when they may not be directly liable for the actions of their CSPs, it is important that outsourcing parties take steps to ensure that their CSPs are willing, capable and sufficiently resourced to meet their obligations under the IPPs.

Tip for CSPs

Before entering into a State contract that confers liability under the PDPA, CSPs should carefully consider whether they are properly equipped and will have sufficient resources to meet their privacy obligations.

If the CSP has not assumed direct liability for their compliance with the IPPs, then any act or practice of the CSP that is an interference with the privacy of an individual will be taken to have also been done or engaged in by the outsourcing party. That is, the outsourcing party, not the CSP, will be liable for any breach. As a result, outsourcing parties must not only ensure that their CSPs are sufficiently resourced and capable of complying with the IPPs, but must also ensure that they have sufficient oversight and contractual levers in place to ensure that their CSPs do in fact comply.

27 For example, see *Privacy Act 1988*, Schedule 3 – National Privacy Principle 6 (Access and Correction), as amended in 2000 by the *Privacy Amendment (Private Sector) Act 2000*.

Tip for CSPs

CSPs not assuming direct liability for their compliance with the IPPs should expect the outsourcing party to be much more prescriptive in relation to IPP compliance. In general, CSPs should expect outsourcing parties to require the same level of oversight and protection of personal information from the CSP as they do from their own staff.

4.2 Training and awareness

Outsourcing parties should consider whether the CSP provides privacy training to its employees, and encourage those that do not, to implement a privacy training program. Training is critical to ensuring that employees who handle personal information are aware of their obligations. Staff who are well versed in privacy are less likely to make errors when handling personal information, minimising the potential for data breaches.

Privacy training is important for employees to complete not only when they first commence their role, but on an ongoing basis.

4.3 Data security (IPP 4 and the VPDSF)

IPP 4 requires an organisation to take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification and disclosure. In general, compliance with the VPDSF (see Step three above) will amount to 'reasonable steps' for the purposes of IPP 4.1.

This means that even outsourcing parties (and CSPs) that do not have an obligation to comply with the VPDSF under Part 4 of the PDPA (for example, local councils) should still use the VPDSF as their primary reference point when determining the steps that may be 'reasonable' to take to protect the personal information they hold.[28]

If a CSP has assumed direct liability for their compliance with the IPPs, they should apply the VPDSF in relation to any personal information they hold. If the CSP has not assumed direct liability for their compliance with the IPPs, the outsourcing party will be responsible for ensuring that reasonable steps are taken by the CSP. Some of the relevant security considerations are outlined above in Step Three. Guidance in relation to the VPDSF is also available on the CPDP website.

4.4 Ensuring personal information is accurate, complete and up to date (IPP 3)

IPP 3 requires an organisation to take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, complete and up to date. CSPs and outsourcing parties should work together to ensure the quality of not only the data they hold, but also the data held by the other party. If it becomes apparent to either party that the information suffers from data quality issues, it is good privacy practice to advise the other party accordingly.

If a CSP has assumed direct liability for their compliance with the IPPs, then they must take reasonable steps to ensure the quality of any personal information that they collect, use or disclose. Outsourcing parties should satisfy themselves that their CSPs are adequately equipped to manage data quality and have appropriate procedures in place. This may involve implementing measures to ensure that data

28 CPDP has produced *Guidelines to protecting the security of personal information: 'Reasonable' steps under Information Privacy Principle 4.1*, available online at: https://www.cpdp.vic.gov.au/images/content/pdf/privacy_guidelines/IPP_4_Guidelines.pdf.

is accurately collected, verified and reviewed, as well as having policies in place to purge old or out of date information, or to put warnings on unreliable information. The *Guidelines to the Information Privacy Principles* contain further information on IPP 3.[29]

If a CSP has not assumed direct liability for their compliance with the IPPs, then the outsourcing party must take reasonable steps to ensure that data quality is maintained. This may include prescribing processes or minimum standards to ensure that information is accurately recorded, unreliable data is identified, and old data is regularly purged.

4.5 Privacy policies (IPP 5)

IPP 5.1 requires an organisation to set out, in a publicly available document, policies on its management of personal information and to make the document available to anyone who asks for it. IPP 5.2 requires organisations let individuals know what sort of information they hold, for what purposes, and how they collect, hold, use and disclose that information, when an individual asks.

If the CSP has assumed direct liability for their compliance with the IPPs, the outsourcing party should take steps to confirm that the CSP has a comprehensive privacy policy in place (or intends to implement one) and should make sure that the existing (or planned) privacy policies of its CSP comply with IPP 5. The policies must be current, accurate and reflect any changes that the outsourcing arrangement creates.

If the CSP has not assumed direct liability for their compliance with the IPPs, they will not need to have a privacy policy themselves. However, the CSP and the outsourcing party should work together to ensure that the outsourcing party's privacy policy adequately explains its policies and procedures for the management of personal information under the outsourcing arrangement.

The outsourcing party and the CSP's privacy policy should clearly state whether the CSP or the outsourcing party is responsible for compliance with the IPPs in relation to the outsourced services, and who is responsible for managing complaints.

4.6 Collection notices (IPP 1)

IPP 1.3 requires organisations collecting personal information about an individual to take reasonable steps to ensure that the individual is aware of:

- the identity of the organisation and how to contact it
- their ability to access and correct the information
- the purpose of collection
- to whom the CSP usually discloses the information
- any laws requiring the CSP to collect the information
- any consequences for individuals if they do not provide their personal information.

This is known as a 'collection notice' or 'giving notice'.

If the CSP has assumed direct liability for their compliance with the IPPs, then they will be responsible for giving notice when they are collecting personal information from individuals directly. The outsourcing party should take steps to confirm that its CSP is aware of the requirements of IPP 1.3, and that the CSP has, or will establish, processes to make sure the required notice is given to individuals.

29 See https://www.cpdp.vic.gov.au/images/content/pdf/privacy_guidelines/OVPC%20Guidelines%20to%20the%20IPPs%20Edition%203%202011.pdf.

If the CSP has not assumed direct liability for compliance with the IPPs, the outsourcing party will be responsible for any failure by the CSP to give adequate notice when collecting personal information. Outsourcing parties should ensure that their outsourcing arrangements provide them with sufficient contractual mechanisms for ensuring that appropriate notice is provided by their CSPs when they collect personal information.

However, not all outsourcing arrangements involve the CSP collecting personal information directly from individuals. For example, if the outsourcing arrangement is such that the outsourcing party is to collect personal information from individuals and subsequently disclose it to its CSP, the outsourcing party will need to give notice to individuals and identify the CSP as an organisation to whom it usually discloses personal information. A CSP who has assumed liability may also need to consider the application of IPP 1.5, which requires an organisation to take reasonable steps to give notice of indirect collection to individuals, where their personal information has been, or will be, collected from another source.

4.7 Transferring personal information to and from the CSP (IPP 2)

An outsourcing party should ensure that any transfer of personal information complies with the IPPs. In particular, disclosure of personal information to the CSP by the outsourcing party must be consistent with IPP 2. As noted above in Step 4.6, affected individuals should also be notified at the time of collection that their personal information will be disclosed to the CSP (IPP 1.3).

Where disclosure of personal information to the CSP is permitted under IPP 2, the outsourcing party should ensure that the transfer occurs securely, and that reasonable steps will be taken to protect personal information from misuse or loss (in accordance with IPP 4 and the VPDSF).

Example – Transfer of personal information to a CSP

A local council delivers meals to elderly residents, and decides to introduce a home cleaning service for the same residents. The council intends to engage a CSP to carry out the proposed cleaning service. The council collected residents' personal information for the purpose of delivering the meal service program, and must comply with IPP 2 if it wants to transfer this information to the CSP for the purpose of carrying out the cleaning service. Because the disclosure is for a different purpose to that for which the information was originally collected, the council will need to obtain the residents' consent to use their information for a secondary purpose.

4.8 Sensitive information (IPP 10)

IPP 10 imposes additional restrictions on when and how outsourcing parties and their CSPs can collect *sensitive information*. Where a CSP may have reason to collect sensitive information during the course of an outsourcing arrangement:

- If the CSP has assumed direct liability for their compliance with the IPPs, the outsourcing party should take steps to confirm that the CSP is aware of the additional requirements of IPP 10, and will comply with them.
- If the CSP has not assumed direct liability for their compliance with the IPPs, the outsourcing party should ensure that measures are in place to prevent the CSP from collecting sensitive information contrary to IPP 10.

Further, additional controls may be required under the VPDSF to limit access and prevent unauthorised access to certain types of information (whether personal information or not).

4.9 Access and correction (IPP 6)

Under IPP 6, a CSP is required to provide individuals with access to the personal information it holds about them, upon request.

Outsourcing parties must consider the manner in which access and correction will be provided. If the CSP has assumed direct liability for their compliance with the IPPs, the obligation to provide access or correction will fall on them. Nevertheless, outsourcing parties should confirm their CSPs have appropriate procedures in place to facilitate this, and satisfy themselves that their CSPs will be compliant.

If the CSP has not assumed direct liability for their compliance with the IPPs, then it will remain the responsibility of the outsourcing party to respond to an access or correction request, even where the relevant information is held by the CSP. Appropriate arrangements should be addressed in the State contract, for example by providing that:

- the CSP will provide individuals with access to their personal information and facilitate requests for correction in line with IPP 6, so individuals can make requests directly to the CSP, and/or
- the CSP will comply with any requests made by the outsourcing party for the purpose of complying with IPP 6, within specified timeframes, so that individuals can make requests to the outsourcing party and the outsourcing party is able to comply.

4.10 Complaint handling

An outsourcing party and its CSP must decide how privacy enquiries and complaints will be dealt with, including which party will be responsible for responding to an enquiry. Such matters should be made clear to potential complainants (in privacy policies and collection notices) so they know where to direct their complaint. Outsourcing parties may also wish to consider the obligations their CSPs will have to assist them in responding to complaints about the CSP's acts or practices.

If the CSP has assumed direct liability for compliance with the IPPs, the PDPA allows complaints to be made against the CSP itself. As a result, the CSP must have appropriate processes in place to manage and resolve complaints.

If the CSP has not assumed direct liability for compliance with the IPPs, complaints must be made against the outsourcing party. In order to be able to adequately respond to any complaints, the outsourcing party will need to have agreed procedures with its CSP so they can investigate and resolve any issues within the required legislative timeframes. Outsourcing parties and CSPs may need to negotiate the terms of such an arrangement – whether it is charged for and at what rate, timeframes for delivery, or other matters such as indemnities, or undertakings to take remedial action. This may mean specific obligations written into the State contract, or it may be covered in a service level agreement or work specification.

4.11 Handling privacy breaches

An outsourcing party should consider how it will respond in the event of a privacy breach.

Points to consider include:

- Will the CSP be required to notify the outsourcing party?
- Will the outsourcing party be able to direct the CSP to take action to mitigate any consequences?
- Will the CSP be required to notify CPDP in the event of a breach?
- Will a specific contact be appointed for complaints arising from the breach?

For more information on dealing with privacy breaches, see the *Responding to privacy breaches guidelines*.[30]

Tip for CSPs

As noted at 3.3 above, breaches happen. In most cases, it is the way that the CSP handles the breach, rather than the fact that the breach occurred, that has the biggest impact on the outsourcing party's trust and confidence going forward. Promptly reporting breaches and working closely with the outsourcing party to mitigate any consequences and prevent re-occurrences is likely to lead to a stronger client relationship.

4.12 Handling personal information at the end of a contract

An outsourcing party should consider how a CSP is to handle personal information at the conclusion of a contract. IPP 4.2 requires that organisations take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. This is consistent with the VPDSF, under which outsourcing arrangements should require CSPs to return or dispose of any public sector data that is not publicly available upon completion or termination of the arrangement.

Outsourcing parties should ensure that all personal information is either returned or properly disposed of at the conclusion of the contract as outlined in Steps 3.6 and 3.9 above. Any recordkeeping requirements under the PRA should also be taken into account.

30 See https://www.cpdp.vic.gov.au/images/content/pdf/privacy_guidelines/OVPC%20Responding%20to%20Privacy%20Breaches%20Guideline%20May%202008.pdf.

Step Five — Ongoing steps during performance of the contract

5.1 Ongoing monitoring and assurance

While pre-contractual steps are important, an outsourcing party will have an ongoing responsibility for the official information held by its CSP, and must continue to ensure that data security and privacy obligations are met during the life of the State contract.

In order to do this effectively, outsourcing parties should work collaboratively with their CSPs to actively identify and mitigate privacy and security risks throughout the life of the arrangement. The preceding sections have focused on specifying the legal rights and obligations of each party, and while it is valuable to have these clearly defined, legal action against a CSP should always be a last resort. Active and collaborative risk management will always be more effective than reactive sanctions.

This means that outsourcing arrangements can't just be 'set and forget' exercises. Outsourcing parties should make sure they have appropriate measures in place to ensure that they, and their CSPs, are meeting their obligations under the VPDSF and the IPPs.

Outsourcing parties should subject the acts and practices of their CSPs to at least the same level of ongoing scrutiny in relation to privacy and data security as they would their internal acts or practices. This may mean:

- regular surveys, reports, site visits and/or audits are conducted on how the CSP is handling official information
- regular reviews of the outsourcing arrangement as a whole from a privacy and data security perspective, including regular re-assessment of risks and associated mitigation strategies
- responding to requests for assistance or advice from their CSPs about their privacy and data security obligations, and working with CSPs to respond to data breaches and/or manage security incidents.

Additionally, any major changes to the outsourcing arrangement or the way in which the outsourced services are provided should be reviewed from a privacy and data security perspective.

Step Six — At the conclusion of the contract

6.1 Destruction or transfer of the official information held by the CSP

When conducting their IPPs and VPDSF due diligence, outsourcing parties should have considered and provided for the appropriate handling of official information at the conclusion of the contract. An outsourcing party should ensure that these provisions are carried out when the contract ends.

Unless there are specific destruction provisions in place, all copies of information should be returned to the outsourcing party. Any disposal of information must be consistent with the recordkeeping requirements set out by PROV under the PRA.

It may not be possible to fully remove the outsourcing party's data from the CSP's ICT system. However, sanitisation should be undertaken to the extent possible at the conclusion of the contract. Outsourcing parties should require CSPs to provide attestation of the disposal or return of all their data.

6.2 Final audit/report from the CSP

An outsourcing party should consider performing a final audit or require a final report from its CSP to make sure all official information has been securely returned or disposed of and is accounted for. Failing to account for all information can pose significant data security, privacy and reputational risks. Conducting a robust final audit reduces the risk of information being abandoned and then improperly accessed (for example, where a file is later discovered in garbage disposal).

6.3 Renewing and extending contracts

Where a contract is to be renewed or extended, an outsourcing party should review the contract to ensure it adequately deals with existing or new privacy and data security obligations. If required, the contract should be amended accordingly. Failure to properly renew a contract may mean that the CSP is no longer required to comply with privacy and data security requirements, and the outsourcing party could be liable for a breach.

Glossary

Availability: the desired state that allows authorised persons to access defined information for authorised purposes at the time they need to do so.

Business Impact Level (BIL): numerical measures of scaled consequences, identifying the potential impact arising from a compromise to the confidentiality, integrity or availability of information. BILs are also referred to as a consequence table.

Confidentiality: 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.

Contracted service provider (CSP): a person or body who provides services under a State contract.

Dissemination Limiting Marker (DLM): a protective marking that indicates access to official information should be limited. DLMs are to be used when a security assessment of potential compromise of confidentiality of the information identifies that disclosure is limited or prohibited by legislation, or where special handling is required and dissemination of the information needs to be controlled.

Information privacy: refers to an individual's right to determine for themselves who has access to their personal information and how it is used.

Information Privacy Principles (IPPs): 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.

Integrity: the assurance that official information has been created, amended or deleted only by the intended authorised means and is correct and valid.

Official information: a term used in this document to refer to both *public sector data* and *personal information*.

Outsourcing: the contracting out of functions or activities.

Outsourcing party: an organisation that contracts out the performance of functions or activities to another person or body.

Personal information: 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.

Protective data security: 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.

Public sector body: a term used in this document to collectively refer to organisations to which Part 3 of the PDPA applies, and agencies and bodies to which Part 4 of the PDPA applies.

Public sector data: any information (including personal information) obtained, received, or held by an agency or body to which Part 4 [of the PDPA] applies.

Sensitive information: defined in the *Privacy and Data Protection Act 2014* as information or an opinion about an individual's –

(a) racial or ethnic origin; or
(b) political opinions; or
(c) membership of a political association; or
(d) religious beliefs or affiliations; or
(e) philosophical beliefs; or
(f) membership of a professional or trade association; or
(g) membership of a trade union; or
(h) sexual preferences or practices; or
(i) criminal record – that is also personal information.

State contract: a contract between an organisation (as defined in s. 3 of the *Privacy and Data Protection Act 2014*), person, agency or body (to which Part 4 or 5 of the *Privacy and Data Protection Act 2014* applies), and another person or body under which services are provided to one party (the outsourcing party) by the other party (the contracted service provider) in connection with the performance of the functions of the outsourcing party.

Subcontracting: when a contracted service provider subsequently outsources the functions or activities they have been engaged to provide to the original outsourcing party.

Victorian Protective Data Security Framework (VPDSF): 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*.

Victorian Protective Data Security Standards (VPDSS): 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 VPDSF.

This page is intentionally left blank.

This page is intentionally left blank.

Commissioner for Privacy and Data Protection

VICTORIA State Government