



# 2026 | Committees of management of Crown land reserves

## Protective Data Security Plan

Version 1.0

Committee of management name: \_\_\_\_\_

### Before you start

- Please refer to the *Committee of management Protective Data Security Plan (PDSP) How-to Guide* for help filling out this form.
- A **completed copy of this Plan is due** to the Office of the Victorian Information Commissioner (OVIC) **by 31 August 2026**.
  - Please ensure you **maintain a completed copy** of this plan for your own records.
- This document has been marked as **OFFICIAL** by OVIC. If you feel your Committee's PDSP requires a different marking, please contact us.
- Should you require assistance in completing this form, please call **1300 006 842** or email **security@ovic.vic.gov.au**

## Contents

Document Details .....	3
<b>PART A – Contact information (mandatory)</b> .....	5
<b>PART B – Self-assessment against the requirements (mandatory)</b> .....	6
Requirement 1 .....	6
Requirement 2 .....	7
Requirement 3 .....	8
Requirement 4 .....	9
Requirement 5 .....	10
Requirement 6 .....	11
Requirement 7 .....	12
Requirement 8 .....	13
Requirement 9 .....	14
Requirement 10 .....	15
Requirement 11 .....	16
Requirement 12 .....	17
Requirement 13 .....	18
Requirement 14 .....	19
Commentary section (Optional).....	20
<b>PART C – Attestation (mandatory)</b> .....	21
<b>PART D – Reporting on behalf of multiple committees of management</b> .....	22

Document Details

Version	Publish date	Amendments in this version
1.0	December 2025	Initial version for committees of management of Crown land reserves

How will the information in the PDSP be used and managed?

In-line with OVIC’s functions under the PDP Act, content from PDSP submissions may form the basis of reporting back to organisations and the Victorian Government including the Victorian Government Chief Information Security Officer.

OVIC will collect some personal information as part of the PDSP form including the name and contact details of the public sector body Head and nominated contact (Information Security Lead). OVIC will use this information to communicate with these contacts about the PDSP, broader security initiatives and activities, distributing information security-related content, or collecting feedback.

OVIC will not disclose personal information without consent, except where required to do so by law. For more information about how OVIC handles personal information, please see OVIC’s Privacy Policy.

The information provided in the PDSP will be managed in accordance with the protective marking assigned. The contents of the PDSP are exempt from the *Freedom of Information Act 1982* (Vic).

## Information security

Under the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**), committees of management are responsible for protecting the information they generate, hold and manage, ensuring the right people have access to the right information at the right time. This includes securing systems that hold or transmit this information.

### Legislative information security obligations

Under Part 4 of the PDP Act<sup>1</sup> a committee of management (**CoM**) must ensure that:

- it does not do an act or engage in a practice that contravenes a [Victorian] protective data security standard (**VPDSS** or **Standard**), in respect of public sector data [CoM information] collected, held, managed, used, disclosed or transferred by it and public sector data systems [CoM systems] kept by it.
- a contracted service provider [third party] of the agency or body does [the CoM] not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider for the agency or body.
- a security risk profile assessment is undertaken for it, including an assessment of any contracted service provider of the agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body.
- a protective data security plan (**PDSP**) is:
  - developed that addresses the Standards applicable to that agency or body.
  - developed that also addresses compliance by any contracted service provider of the agency or body with the protective data security standards, to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body.
  - reviewed if there is a significant change in the operating environment or the security risks relevant to the agency or body.
- a copy of the PDSP is given to the Information Commissioner.

### Addressing the Standards as a CoM

As outlined, a CoM is required to develop and submit a copy of its completed PDSP. A PDSP outlines the minimum information security measures a CoM will implement to ensure its information and systems are managed in a risk-informed way. OVIC has developed a PDSP template and ‘How-to’ guide specifically for CoMs.

### Mapping the Standards to the CoM requirements

This PDSP form contains 14 tailored ‘requirements’ for CoMs that map back to the VPDSS. By submitting this PDSP addressing the 14 requirements, the obligation under section 89 of the PDP Act to develop, review and submit a PDSP that addresses the Standards will be fulfilled. For further information, please read OVIC’s *How-to Guide: Protective Data Security Plan for Committees of Management of Crown land reserves*.

### Incidents impacting CoM information and systems

OVIC encourages CoMs to contact our office if they are impacted by an information security incident that adversely affects CoM information or systems.

---

<sup>1</sup> For the full list of requirements, see section 88 and 89 of the PDP Act.

PART A – Contact information (mandatory)

	Chairperson	Person authorised by the Chairperson to submit a copy of this PDSP	Nominated point of contact (if different from the Chairperson)
Full name			
Position title	Chairperson		
Phone number			
Email address			
Postal address			

# PART B – Self-assessment against the requirements (mandatory)

## Requirement 1

The committee of management records how it securely manages its information.

*This requirement maps to Standard 1 of the VPDSS*

*An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.*

Explanation of requirement	Recommended supporting activity
Documentation informs all committee members (current and future) on the expectations around securely managing committee information.	Committee members discuss and write down their approach to securely managing committee of management of Crown land reserve (CoM) information.  This could be recorded in the form of a simple statement, or for more complex CoMs, it may be recorded in one or more documents.

### Action required – complete the below

Current Response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

## Requirement 2

The committee of management identifies and records the different types of information it manages.

*This requirement maps to Standard 2 of the VPDSS     An organisation identifies and assesses the security value of public sector information.*

### Explanation of requirement

CoMs manage different kinds of information, such as:

- asset registers
- meeting agendas and minutes
- decision-making documentation and correspondence
- financial statements, invoices, and receipts
- policies and procedures
- instruments of delegation
- employee records
- maps

Sometimes these are kept in paper or electronic form.

Identifying and documenting the different types of information that committee members manage helps build community confidence.

### Recommended supporting activity

Committee members discuss the various information types managed by the CoM. This will help the CoM identify the different information it manages.

Members should then create a summarised record of these information types, noting these down in either a hard copy or electronic (digital) format.

OVIC has developed a template for CoMs to document these actions. This template is referred to as an Information Asset Register. CoMs are encouraged to use this template to identify and record their information.

- A copy of this template is available on the OVIC website. Please navigate to <https://go.vic.gov.au/4pScREm> where you can download this resource.
- If you require assistance please contact OVIC at [security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au) or 1300 006 842.

### Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

### Requirement 3

The committee of management identifies and records sensitive information it manages.

*This requirement maps to Standard 2 of the VPDSS      An organisation identifies and assesses the security value of public sector information.*

#### Explanation of requirement

To ensure CoM information is properly protected, members need to identify and record material that is sensitive in nature. This will help committee members maintain the confidentiality of the material they are managing on behalf of the community.

For instance, some information types may have more sensitive components to them, e.g. volunteer records may have components that the committee members are authorised to disclose, but there may be other components of these same volunteer records that need to remain confidential – i.e. details of addresses, credit card details, Workcover claims etc.

#### Recommended supporting activity

Committee members review the CoM Information Asset Register to identify specific information types (contents) that are considered confidential or sensitive (i.e. not for public distribution).

Members should then update the CoM Information Asset Register, recording which information has sensitive components associated with it.

When reviewing the CoM information, consider what would happen if:

- an unauthorised person accessed this material, or
- it was disclosed to someone who wasn't supposed to see or hear it?

Think about what steps you could take to manage these risks.

#### Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+



## Requirement 4

The committee of management identifies and records information that needs to be accurate and available when used.

*This requirement maps to Standard 2 of the VPDSS     An organisation identifies and assesses the security value of public sector information.*

### Explanation of requirement

To ensure CoM information is properly maintained, committee members need to keep up-to-date records. This will help committee members manage the accuracy and availability of the material they hold on behalf of the community.

**Accuracy (integrity)** - If CoM records are inaccurate or incomplete, committee members may find themselves unable to provide the correct information when requested.

*For example* – The CoM is unable to correctly advise on the boundaries of native title on managed land.

**Availability** - If CoM records are unavailable, committee members may find themselves unable to provide information when called upon.

*For example* – A committee member had sole custody of a master CoM record and is no longer able to find it, resulting in advice not being able to be provided.

### Recommended supporting activity

Committee members review their Information Asset Register to identify specific information / records that require careful management to ensure it remains accurate and available.

Members should then update their CoM Information Asset Register, recording which information is essential (i.e. relied upon by committee members for its continued accuracy and availability).

When reviewing the information, consider what would happen if:

- unauthorised adjustments, modifications or changes were made to the information?
- it was unavailable when the information was called upon?

Think about what steps you could take to manage these risks.

### Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

# Requirement 5

The committee of management documents any information security risks relating to the management of its information.

*This requirement maps to Standard 3 of the VPDSS*      *An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks.*

## Explanation of requirement

The CoM documents information security risks associated with the CoM material they manage on behalf of the community.

By understanding and documenting these risks, the CoM can prioritise its efforts and resources.

## Recommended supporting activity

Committee members may already have a register of risks for their CoM, stored in paper or electronic (digital) form. This activity supports existing guidance set out by DEECA under Chapter 6 (Risk Management and Organisational Planning) of the Committee of Management Guidelines.

Requirement 5 calls on committee members to simply update this existing register with any information security risks identified in your discussions.

*For example – An information security risk that may be recorded in your register could be “The risk of CoM documents being destroyed, caused by a fire (no backups available), resulting in lack of confidence from the local community in the management of the CoM”.*

The CoM may seek to manage this risk by creating copies of its records and storing these copies away from originals.

## Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

## Requirement 6

The committee of management validates who (people) and what (systems) have direct access to its information.

*This requirement maps to Standard 4 of the VPDSS*      *An organisation establishes, implements and maintains an access management process for controlling access to public sector information.*

### Explanation of requirement

The CoM ensures only the right people and systems are granted direct access to CoM information, when and where appropriate. The *right*:

- *people* may include, but are not limited to, authorised employees or volunteers performing certain roles for the CoM, individuals from neighbouring CoMs, or private organisations providing support or assistance to the CoM.
- *systems* may include, but are not limited to, internal or external IT systems that have been authorised to process and/or store CoM information (e.g. computer, server, email system).

CoMs are expected to ‘validate’ (confirm / approve) the legitimacy of these people and systems before granting direct access to CoM information. This includes external organisations and/or systems. Members of the CoMs should clarify how the committee’s information will be used by these individuals and/or systems.

### Recommended supporting activity

Committee members discuss, verify and document who (people or organisations) and what (systems – if any) should be granted access to committee information. For example, consider:

- which committee roles are authorised to directly access certain information, and which roles should be restricted from accessing the same material?
- how the CoM will validate requests from third parties, such as community members, private industry groups and/or systems, taking into account whether the requests for access are legitimate and permitted by law /regulation?

### Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

Requirement 7

The committee of management documents the roles and responsibilities for those managing committee information.

*This requirement maps to Standard 5 of the VPDSS*      *An organisation ensures all persons understand their responsibilities to protect public sector information.*

Explanation of requirement

The CoM:

- has documented expectations around the handling and management of committee information.
- ensures everyone understands their role and responsibilities when managing information on behalf of the community.

Recommended supporting activity

Committee members discuss and document the roles and responsibilities of personnel that handle and manage committee information. Consider:

- what roles are responsible for what types of information
- whether CoM members know what information they are allowed to disclose, and in what circumstances
- how the CoM will communicate these expectations to personnel.

Personnel may include:

- volunteers
- individual committee members
- staff
- third parties (sub-contractors).

Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

### Requirement 8

The committee of management manages any compromises (incidents) to its information.

*This requirement maps to Standard 6 of the VPDSS*

*An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.*

Explanation of requirement	Recommended supporting activity
<p>The CoM has documented expectations around the handling and management of situations where committee information has been compromised.</p> <p>To help reduce the impact of an information security incident (i.e. where committee information has been adversely affected) CoMs should refer to a documented plan.</p> <p>Information security incident examples can include scenarios where:</p> <ul style="list-style-type: none"><li>sensitive information has been mistakenly released to a member of the public via an enquiry (e.g. giving out contact details) where this wasn't permitted by relevant laws or regulations</li><li>committee information has been stolen, lost or damaged.</li></ul>	<p>Committee members discuss and document how they will deal with a variety of information security incidents.</p> <p>It's important to think through different scenarios and have a plan in place to manage incidents that have the potential to affect the confidentiality, integrity and/or availability of committee information. For example, in the event of an incident:</p> <ul style="list-style-type: none"><li>What steps would you need to take?</li><li>Who would you notify of the incident? E.g., OVIC, DEECA, Victoria Police</li><li>Who will manage the incident?</li><li>Who can you turn to for help?</li><li>Where is the committee's incident management plan?</li></ul>

Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

### Requirement 9

The committee of management documents how it intends to protect its information in the event of a disaster.

*This requirement maps to Standard 7 of the VPDSS     An organisation embeds information security continuity in its business continuity and disaster recovery processes and plans.*

Explanation of requirement	Recommended supporting activity
<p>The CoM has documented expectations around the handling and ongoing management of committee information in situations where the operations of the committee have been adversely impacted. Examples of this could include:</p> <ul style="list-style-type: none"><li>• a natural disaster such as fire or flood</li><li>• system outages</li><li>• unplanned liquidation or discontinuation of a service offered by a third party.</li></ul>	<p>Committee members discuss and document how the CoM would continue to keep its information secure if the operations of the committee were severely undermined or impacted. Take into account information stored in both hard copy and electronic (digital) format.</p> <p>For example:</p> <ul style="list-style-type: none"><li>• have committee members considered creating secure copies or backups of the committee’s information?</li><li>• where are these copies securely stored? Are they stored away from the normal office/home environment, separate from the originals?</li><li>• would these copies be available following an accident or disaster?</li></ul>

Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

## Requirement 10

The committee of management documents how non-committee members access and/or use its information in a secure way.

*This requirement maps to Standard 8 of the VPDSS      An organisation ensures that third parties securely collect, hold, manage, use, disclose or transfer public sector information.*

### Explanation of Requirement

The CoM has documented its expectations around the secure handling and ongoing management of committee information by non-committee members, including establishing clear expectations around what is required of them when accessing or using its information.

### Recommended supporting activity

CoM members discuss and document:

- who is authorised to access the CoM information?  
(e.g., DEECA, Victoria Police, Local Council, members of the public)
- in what circumstances this access is permitted / authorised
- how the information will be provided to non-committee members
- the various protections required when sharing this information.

### Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

# Requirement 11

The committee of management notifies OVIC of any compromises (incidents) to its information.

*This requirement maps to Standard 9 of the VPDSS*

*An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (VPDSS) and reports to the Office of the Victorian Information Commissioner (OVIC).*

Explanation of requirement	Recommended supporting activity
<p>The CoM ensures OVIC is made aware of any issues impacting the security of its information.</p> <p>To ensure the continued security of CoM information, the confidentiality, integrity and/or availability of this material must be maintained. If any of these attributes are ever compromised, an information security incident may have occurred.</p> <p>An example of an information security incident may be where:</p> <ul style="list-style-type: none"><li>a committee member mistakenly discloses sensitive information (confidentiality)</li><li>committee records have been altered to misrepresent land boundaries (integrity)</li><li>an asset register goes missing (lack of availability)</li></ul>	<p>Committee members discuss and document:</p> <ul style="list-style-type: none"><li>potential types of incidents that may impact CoM information</li><li>who would notify OVIC and in what circumstances</li><li>how they would notify OVIC.</li></ul> <p>Remember, if the confidentiality, integrity and/or availability of CoM information has been compromised, it is likely that an information security incident may have occurred.</p> <p>If you require assistance, please contact OVIC.</p>

## Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+



### Requirement 12

The committee of management members are checked prior to, and throughout, their appointment.

*This requirement maps to Standard 10 of the VPDSS*     *An organisation establishes, implements and maintains personnel security controls addressing all persons continuing eligibility and suitability to access public sector information.*

Explanation of requirement	Recommended supporting activity
<p>The CoM ensures that its members are eligible and suitable to manage committee information.</p> <p>CoMs are responsible for conducting interviews and referee checks prior to endorsing applications for appointment. In addition to this, the Department of Energy, Environment and Climate Action (<b>DEECA</b>) requires minimum probity checks to be conducted prior to appointment, as well as National Criminal Record checks for certain committees.</p> <p>CoMs should ensure members remain eligible and suitable to access, use and handle committee information on an ongoing basis.</p>	<p>Committee members discuss and document the requirements for validating the eligibility and suitability of individuals prior to, and during, their appointment. Committee members refer to this documentation when conducting checks.</p> <p>The CoM will notify DEECA if it believes a member has become unsuitable to continue as a committee member.</p>

Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

Requirement 13

The committee of management securely maintains computer systems that process and/or store its information.

*This requirement maps to Standard 11 of the VPDSS      An organisation establishes, implements and maintains Information Communications Technology security controls.*

Explanation of requirement	Recommended supporting activity
<p>If the CoM uses computer systems / devices to process or store committee information, committee members must ensure these systems/devices are secure.</p> <p>This requirement extends to arrangements where the CoM is using a third party (contracted service provider) to help administer committee operations on its behalf.</p> <p>Where a third party uses a computer system or device to process/store CoM information, the committee must be comfortable with their security arrangements.</p> <ul style="list-style-type: none"><li>• Systems may include cloud-based programs run by a vendor, or programs managed on a local desktop computer or laptop.</li><li>• Devices can include desktop computers, laptops, smart phones, tablets, iPads, etc.</li></ul> <p>Only select “not applicable” if the committee is not using computer systems or devices to process and/or store committee information.</p>	<p>CoM members discuss and document the requirements for ensuring any computer systems (including cloud-based systems) or devices processing/storing committee information are secure.</p> <p>CoM members may consider:</p> <ul style="list-style-type: none"><li>• updating software on any systems / devices</li><li>• using strong passwords</li><li>• backing up systems / devices</li><li>• using anti-virus software</li><li>• being mindful of any links members may click on (e.g., phishing attempts, scams.)</li><li>• using multi-factor authentication methods (where offered)</li></ul>

Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

Requirement 14

The committee of management maintains its facilities, equipment and services that help securely manage its information and systems.

*This requirement maps to Standard 12 of the VPDSS    An organisation establishes, implements and maintains physical security controls addressing facilities, equipment and services.*

Explanation of requirement	Recommended supporting activity
<p>The CoM ensures its hardcopy and softcopy information is physically protected in various forms. This includes using physical security controls for any:</p> <ul style="list-style-type: none"><li>• facilities (buildings) where committee information or systems are handled or stored</li><li>• equipment used to store or manage committee information or systems</li><li>• services that help monitor or protect locations or facilities where committee information or systems are stored.</li></ul>	<p>Committee discuss and document the requirements for maintaining physical security controls designed to protect committee information. Physical measures may include:</p> <ul style="list-style-type: none"><li>• facilities – e.g., locks on doors, alarms</li><li>• equipment – e.g., types of containers that are used to store information, such as locked cabinets, safes, protective containers or boxes (to avoid water or insect damage)</li><li>• services – e.g., security guard, monitoring companies where applicable.</li></ul>

Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

## Commentary section (Optional)

Please use the space below if you wish to provide any additional information or commentary on the committee of management or the 14 requirements.

## PART C – Attestation (mandatory)

The attestation must be signed by the Chairperson of the committee of management of Crown land reserves (**CoM**) or their authorised representative (as specified in Part A of this form).

This Protective Data Security Plan is submitted to the Victorian Information Commissioner in accordance with section 89 of the *Privacy and Data Protection Act 2014* (Vic).

I, \_\_\_\_\_ attest that \_\_\_\_\_  
(Full Name) (Name of the CoM)

- has implemented the 14 requirements, or is in the process of planning and/or implementing these requirements (where applicable), as required by the Victorian Protective Data Security Standards,
- the contents of this PDSP accurately reflect the current information security risks and program of the CoM, and
- I am aware of, and acknowledge, my trust's obligations under Part 4 of the PDP Act.

I am authorised to make this attestation.

Signature

\_\_\_\_\_

Print name

\_\_\_\_\_

Position

\_\_\_\_\_

Date

\_\_\_\_\_

☐ Check this box if more than one CoM is captured by this PDSP.

(Ensure you list the details of the additional CoMs in **Part D of this form**)

## PART D – Reporting on behalf of multiple committees of management

The committees of management of Crown land reserves listed in this section have **the same**:

- risk profiles
- types of information
- security practices and
- responses to each of the 14 requirements

and have authorisation from the Chairperson of the committee of management to be included in this submission.

Name of committee of management	Name of the Chairperson	Committee of management phone number <u>and</u> email address	The Chairperson of the committee of management has authorised the submission of this PDSP on their behalf
			<input type="checkbox"/> (check box)
			<input type="checkbox"/> (check box)
			<input type="checkbox"/> (check box)
			<input type="checkbox"/> (check box)
			<input type="checkbox"/> (check box)