

Victorian Protective Data Security Standards

Version 2.0 (2019) to Version 1.0 (2016) Mapping

Standard #	Previous Standard # (VPDSS 1.0)	Statement of Objective
1 Information Security Management Framework	Standard 1 – Security Management Framework Standard 3 – Policies and Procedures Standard 12 - Compliance (COM-020 only)	To clearly establish, articulate, support and promote the security governance arrangements across the organisation and manage security risks to public sector information.
2 Information Security Value	Standard 13 – Information Value Standard 14 – Information Management	To ensure an organisation uses consistent identification and assessment criteria for public sector information across its lifecycle to maintain its confidentiality, integrity and availability.
3 Information Security Risk Management	Standard 2 – Security Risk Management Standard 11 – Security Plans	To ensure an organisation manages information security risks through informed business decisions while applying controls to protect public sector information.
4 Information Access	Standard 4 – Information Access	To formally authorise and manage the physical and logical access to public sector information.
5 Information Security Obligations	Standard 5 – Security Obligations Standard 6 – Security Training and Awareness	To create and maintain a strong security culture by ensuring that all persons understand the importance of information security across all the security areas and their obligations for protecting public sector information.

<p>6 Information Security Incident Management</p>	<p>Standard 7 – Security Incident Management</p>	<p>To ensure a consistent approach for managing information security incidents, in order to minimise harm/damage to government operations, organisations or individuals.</p>
<p>7 Information Security Aspects of Business Continuity and Disaster Recovery</p>	<p>Standard 8 – Business Continuity Management</p>	<p>To enhance an organisation’s capability to prevent, prepare, respond, manage and recover from any event that affects the confidentiality, integrity and availability of public sector information.</p>
<p>8 Third Party Arrangements</p>	<p>Standard 9 – Contracted Service Providers Standard 10 – Government Services Standard 15 – Information Sharing</p>	<p>To confirm that the organisation’s public sector information is protected when the organisation interacts with a third party.</p>
<p>9 Information Security Reporting to OVIC</p>	<p>Standard 12 - Compliance</p>	<p>To promote the organisation’s security capability and ensure adequate tracking of its exposure to information security risks.</p>
<p>10 Personnel Security</p>	<p>Standard 16 – Personnel Lifecycle</p>	<p>To mitigate an organisation’s personnel security risks and provide a consistent approach for managing all persons with access to public sector information.</p>
<p>11 ICT Security</p>	<p>Standard 17 – Information Communications Technology (ICT) Lifecycle</p>	<p>To maintain a secure environment by protecting the organisation’s public sector information through ICT security controls.</p>
<p>12 Physical Security</p>	<p>Standard 18 – Physical Lifecycle</p>	<p>To maintain a secure environment by protecting the organisation’s public sector information through physical security controls.</p>

VPDSS Mapping Visual Aid

