On 11 October 2019, the Honourable Gavin Jennings MLC, Special Minister of State, agreed to revoke the Victorian Protective Data Security Standards issued in July 2016 and agreed to issue these new Victorian Protective Data Security Standards in accordance with sections 86 and 87 of the Privacy and Data Protection Act 2014.

On 28 October 2019, Sven Bluemmel, Victorian Information Commissioner, revoked the Victorian Protective Data Security Standards issued in July 2016 and issued these new Victorian Protective Data Security Standards in accordance with sections 86 and 87 of the Privacy and Data Protection Act 2014.

Victorian Protective Data Security Standards

| **Standard #** | **Standard** | **Statement of Objective** |
| --- | --- | --- |
| **1****Information Security Management Framework** | An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture. | 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** | An organisation identifies and assesses the security value of public sector information. | 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** | An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks. | To ensure an organisation manages information security risks through informed business decisions while applying controls to protect public sector information. |
| **4****Information Access** | An organisation establishes, implements and maintains an access management process for controlling access to public sector information. | To formally authorise and manage the physical and logical access to public sector information. |
| **5****Information Security Obligations** | An organisation ensures all persons understand their responsibilities to protect public sector information. | 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. |
| **6****Information Security Incident Management** | An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture. | To ensure a consistent approach for managing information security incidents, in order to minimise harm/damage to government operations, organisations or individuals. |

| **Standard #** | **Standard** | **Statement of Objective** |
| --- | --- | --- |
| **7****Information Security Aspects of Business Continuity and Disaster Recovery** | An organisation embeds information security continuity in its business continuity and disaster recovery processes and plans. | 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. |
| **8****Third Party Arrangements** | An organisation ensures that third parties securely collect, hold, manage, use, disclose or transfer public sector information. | To confirm that the organisation’s public sector information is protected when the organisation interacts with a third party. |
| **9****Information Security Reporting to OVIC** | 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). | To promote the organisation’s security capability and ensure adequate tracking of its exposure to information security risks. |
| **10****Personnel Security** | An organisation establishes, implements and maintains personnel security controls addressing all persons continuing eligibility and suitability to access public sector information. | To mitigate an organisation’s personnel security risks and provide a consistent approach for managing all persons with access to public sector information. |
| **11****ICT Security** | An organisation establishes, implements and maintains Information Communications Technology (ICT) security controls. | To maintain a secure environment by protecting the organisation’s public sector information through ICT security controls. |
| **12****Physical Security** | An organisation establishes, implements and maintains physical security controls addressing facilities, equipment and services. | To maintain a secure environment by protecting the organisation’s public sector information through physical security controls. |