



Victoria Government Gazette

No. S 431 Tuesday 29 October 2019
By Authority of Victorian Government Printer

Privacy and Data Protection Act 2014

NOTICE OF VICTORIAN PROTECTIVE DATA SECURITY STANDARDS 2019 ISSUED BY THE INFORMATION COMMISSIONER UNDER PART 4, DIVISION 3 OF THE PRIVACY AND DATA PROTECTION ACT 2014

Section 86 of the **Privacy and Data Protection Act 2014** (PDP Act) enables the Information Commissioner to issue protective data security standards that apply to agencies and bodies referred to in section 84(1) of the PDP Act.

The Victorian Protective Data Security Standards 2019 were issued on 28 October 2019.

In accordance with section 16A(1) of the **Subordinate Legislation Act 1994**, the Victorian Protective Data Security Standards are published below.

The Victorian Protective Data Security Standards may also be accessed via the website of the Office of the Victorian Information Commissioner at www.ovic.vic.gov.au

SVEN BLUEMMEL
Information Commissioner

Office of the Victorian Information Commissioner

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.

SPECIAL

Standard #	Standard	Statement of Objective
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.
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.

This page was left blank intentionally

bluestar * **PRINT**

The *Victoria Government Gazette* is published by Blue Star Print with the authority of the Government Printer for the State of Victoria

© State of Victoria 2019

This publication is copyright. No part may be reproduced by any process except in accordance with the provisions of the Copyright Act.

Address all enquiries to the Government Printer for the State of Victoria
Level 2, 1 Macarthur Street
Melbourne 3002
Victoria Australia

How To Order



**Retail &
Mail Sales**

Victoria Government Gazette

Ground Floor, Building 8,
658 Church Street,
Richmond 3121

DX 106 Melbourne



Telephone

(03) 8523 4601



Fax

(03) 9600 0478

email

gazette@bluestargroup.com.au

Price Code A