Office of the Victorian Information Commissioner

Phone: 1300 00 6842
Email: security@ovic.vic.gov.au

INFORMATION FOR AGENCIES AND BODIES

Information Security Leads

Part 4 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) applies to the majority of Victorian Public Sector (**VPS**) agencies or bodies (**regulated organisations**) delivering unique services or functions on behalf of government.

Regulated organisations have an obligation to protect public sector information and systems by adhering to the Victorian Protective Data Security Standards (**the Standards**). Accountability for compliance with the Standards rests with the public sector body Head of the regulated organisation, who requires support from personnel who are appropriately skilled, resourced and empowered.

An information security lead (**ISL**) acts as a central point of contact for OVIC to deliver important information security messages and updates relating to the Victorian Protective Data Security Framework (the **Framework**) and Standards. An ISL can support their public sector body head and help guide the implementation of the Standards on behalf of the organisation by coordinating a Protective Data Security Plan (**PDSP**) submission.

Nominating an information security lead

Element E1.050[1] of the Standards outlines that each public sector body Head should nominate an information security lead (**lead**) for their organisation, and notify OVIC of any changes to the lead. If there are changes, OVIC requests the organisation provide the Information Security Unit an alternative point of contact if they move roles or cease working for the organisation.

Email security@ovic.vic.gov.au with any changes to the ISL.

[1] Standard 1 (Information Security Management Framework), Element E1.050

Collection of personal information

As Information Security Leads, we collect your name, organisation, and email address. This information is collected for the purpose of:

- distributing any communications intended for this list including event invitations and updates
- communicating important information security messages intended for the regulated organisation or body.

We will only use your email address and any other personal information you provide for this purpose and will not disclose your personal information without your consent, except where required to do so by law.

You may contact us to request access to your personal information via enquiries@ovic.vic.gov.au. Please visit our Privacy Policy for more information.

Managing an information security work program and organisational reporting

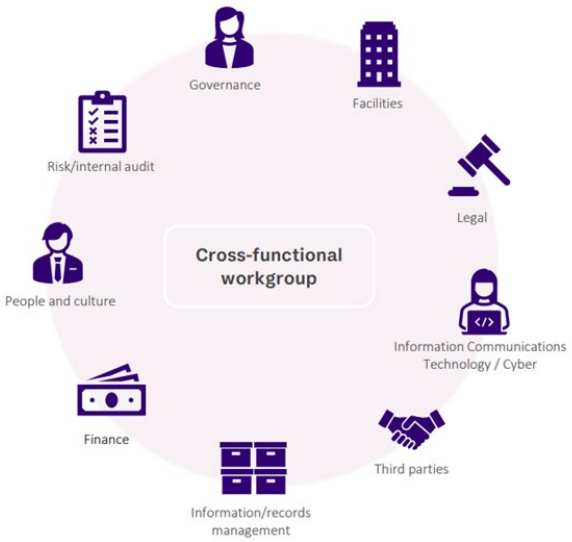
Given the broad nature of the Standards, it is likely that the person coordinating the organisation's information security program will need input and assistance from a wide variety of stakeholders. Where possible, this should include representation from across the business, as well as external bodies and third parties (including contracted service providers). Organisations should take a holistic approach the management of their information security risks and leverage subject-matter experts to help implement aspects of the various Standards and input into the development of a PDSP submission.

Given the diverse nature of the VPS, OVIC does not prescribe a specific role or group that should be tasked with managing information security, or organisational reporting obligations, however an ISL may be well positioned to do so.

Establishing a cross-functional information security committee or workgroup

OVIC encourages organisations to establish a cross functional workgroup with representatives who can contribute subject-matter expertise unique to their security domain or functional work area. This may include specialist knowledge and capabilities drawn from:

- Executive, corporate, legal or procurement groups responsible for addressing security governance requirements, third-party arrangements and contractual arrangements
- Risk managers who assist with integrating information security risks into the organisation's overall risk management framework
- Chief Information Officers (CIOs), information or records managers who assist with identifying information holdings across the organisation
- HR representatives who provide advice and input into personnel security matters



- IT teams that support the delivery of ICT security initiatives
- Internal auditors responsible for managing assurance programs on behalf of the organisation, and
- Facilities managers who provide advice and input into the physical security needs of the business.