Information Protection and Cybersecurity

How we protect your information and manage our cloud data security and compliance.

Information protection is the practice of protecting digital data from unauthorised access, disclosure, alteration and/or destruction. This involves cybersecurity, including technical, administrative and physical measures to safeguard data and ensure the confidentiality, integrity and availability of your information.

Our information-gathering powers and responsibilities

The *Audit Act 1994* governs the Auditor-General's powers and functions, including our access to information during an audit or assurance review, and the standards we must meet. This allows the Parliament, the public sector and the Victorian community to have confidence in us.

As an integrity body, we also have an important responsibility to model best practice in terms of protecting others' information.

What this applies to

Our information-protection responsibilities apply to all information we hold, whether from clients, auditees, other external parties, or our personnel – that is, employees, contractors and consultants, including our external audit service providers (ASPs).

Our approach to information protection

Alignment with trusted standards

We use the Microsoft cloud security benchmark (MCSB) as a single harmonising standard.

Our approach aligns to the Microsoft 365 Zero trust security model, the Victorian Protective Data Security Framework, level 2 of the Australian Cyber Security Centre's Essential Eight Maturity Model, and the Australian Government Secure Cloud Strategy.

Governance framework

The Deputy Auditor-General is the executive sponsor of information protection and leads the application of our information management and security policies, workforce training, continuity of operations, and incident response.

Our digital strategy

Our digital strategy means that we hold information as digital records – we do not collect physical records. This supports strong compliance and monitoring as our systems are configured to create a real-time, highly automated environment.

Zero trust model

Perimeter-based security is no longer enough. Instead, we use the Zero trust security model, applying its 3 principles:

- Zero trust principle 1: Assume breach
- Zero trust principle 2: Never trust, always verify
- Zero trust principle 3: Use least privilege.

Shared responsibility model

While we have overall *accountability* for information protection, our digital strategy uses a shared *responsibility* model.

Shared responsibility with cloud service providers

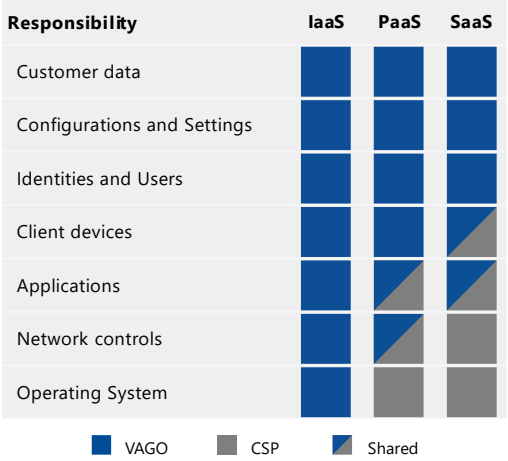
Shared responsibilities

We do not use legacy-based infrastructure in the cloud or on-premises physical infrastructure.

This means we only use Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) solutions.

We are responsible for managing and configuring security and compliance of components we control in the cloud.

Our Cloud Service Providers (CSPs) are responsible for managing the privacy, security and compliance of the cloud. Currently, relevant providers are Microsoft, Kiteworks, Miro and Caseware.



Ensuring compliance by cloud service providers

	Microsoft	Kiteworks	Miro	Caseware
ISO 27001:2013	☑	☑	☑	☑
SOC 2 Type 1 and Type 2	☑	☑	☑	☑
GDPR	☑	☑	☑	
FedRamp	☑	☑		
Australia IRAP	☑	☑		
FIPS 140-2	☑	☑		
HIPAA	☑	☑		
Australia IRAP	☑	☑		
NIST 800-53	☑			

We oversight our CSPs by reviewing their security audits, reports, authorisations and certificates, available at:

- Microsoft's service trust portal
- Kiteworks regulatory compliance
- Miro's trust center
- Caseware Cloud's security certifications.

Ensuring compliance by third-party Audit Service Providers (ASPs)

Our contracts with ASPs contain terms requiring them to manage data in accordance with Protective Data Security Standards and related legislation.

Each year, we seek confirmation from our ASPs that specific controls are operational in their environment/s. We also confirm the currency of any *ISO 27001: Information security, cybersecurity and privacy protection* certifications.

Where an ASP is not *ISO 27001* certified, we undertake periodic assessments of specific MCSB control domains, communicating any non-compliance identified and making relevant recommendations.

Monitoring, assessing and managing risks to information protection

Monitoring, reporting and reviews

We proactively monitor our information protection and cybersecurity risk using the Microsoft Secure Score and MCSB, and we maintain levels of information security that are well beyond industry standards.

- We **monitor** information protection compliance using near real-time performance reporting. Our data analytics shows lead indicators, such as security markings, role access, threats and vulnerabilities.
- We **report** on compliance performance and actions in our monthly Operational Management Group meetings.
- We conduct **reviews** of our implementation plan on a regular basis and of our governance arrangements when there is a major change or at least every 2 years.

Assessing the security value of information

We assess the security value of all information we hold and use automated policies to retain information according to its security value and our legislation.

Based on a business impact assessment of every document, we classify and mark information using 6 visible sensitivities: UNOFFICIAL, PUBLIC, OFFICIAL, OFFICIAL–Sensitive, PROTECTED and SECRET.

Information classified as SECRET

We do not currently manage any SECRET information.

If a situation did require us to collect or hold such information, this would be subject to a management plan developed in consultation with the relevant clients.

Assessing security risks

We periodically undertake security risk assessments as part of our internal audit program. We then proactively manage any resulting actions through our operational governance arrangements and Audit and Risk Committee (ARC).

As information protection and cybersecurity requirements continually evolve, we incorporate planned improvements into our yearly Project Portfolio Planning Framework.

Managing access controls

We authorise and manage all access to information by personnel. This means that personnel only access the information that they require to do their job. This includes administrator privileges.

We manage information access through our systems based on the requirements of each individual's role, which may change over time.

New personnel must …	All personnel must …	For guest users, we …
• verify their identity and qualifications • undergo reference checks • verify their work rights • complete a National Police Check • complete a thorough induction.	• complete a National Police Check every 3 years • disclose any new charges, proceedings or convictions • complete a yearly independence declaration • proactively declare potential conflicts of interest.	review systems access quarterly to: • verify users have appropriate access • remove access when no longer required.

Questions and further information

If you have further questions about the way we protect information or manage cybersecurity more broadly, please contact Christopher Schmidt, Chief Information Officer, christopher.schmidt@audit.vic.gov.au