FACT SHEET

Data Protection

January 2019

VAGO
Victorian Auditor-General's Office

How VAGO secures your information

Introduction

Information and data are critical to the success of VAGO's role to provide authoritative assurance to the Victorian Parliament and community, and is a fundamental foundation to auditing. It helps us plan, execute and report on our audits, and provide relevant insights for public sector agencies to improve their performance.

The *Audit Act 1994* (the Act) underpins this by giving the Auditor-General powers to compel any person to produce any documents. The Act explicitly states that any obligation to maintain secrecy or other restriction on the disclosure of information, where imposed by legislation or Cabinet confidentiality, does not apply. Penalties apply for failing to produce documents in accordance with the Act's requirements. The Auditor-General is accountable for the proper use of this information.

Although our legislative mandate to access information is significant and broad reaching we see it as a mechanism of last resort. We, like you, take our information security responsibilities very seriously and are committed to providing transparency on how we secure your information. This fact sheet is designed to give that transparency.

To enable you to accurately understand our information security posture, we have provided technical detail in lieu of general statements e.g. we say our providers are FIPS 140-2 certified rather than saying data is encrypted at rest.

If you wish to discuss our information security posture further, please contact Dave Barry, Deputy Auditor-General, on dave.barry@audit.vic.gov.au, 03 8601 7133 or 0459 857 018.

VAGO audit staff are not authorised to communicate in detail on our information security posture to reduce the risk of inaccurate information being communicated.

Our strategy

Our approach to information security is aligned with the *Australian Government Secure Cloud Strategy*, which was released in 2017 and is at https://www.dta.gov.au/what-we-do/policies-and-programs/secure-cloud.

Consistent with this strategy, appropriately certified cloud providers are significantly better placed than internal teams to implement and monitor security controls, achieve compliance and have this compliance assessed by independent third parties.

We refer to all information directly sourced from our clients for audit purposes with a classification of UNCLASSIFIED or PROTECTED as high value workloads.

We do not currently manage any CONFIDENTIAL or SECRET workloads. If we needed to acquire these workloads they would be subject to a management plan developed in consultation with the relevant clients.

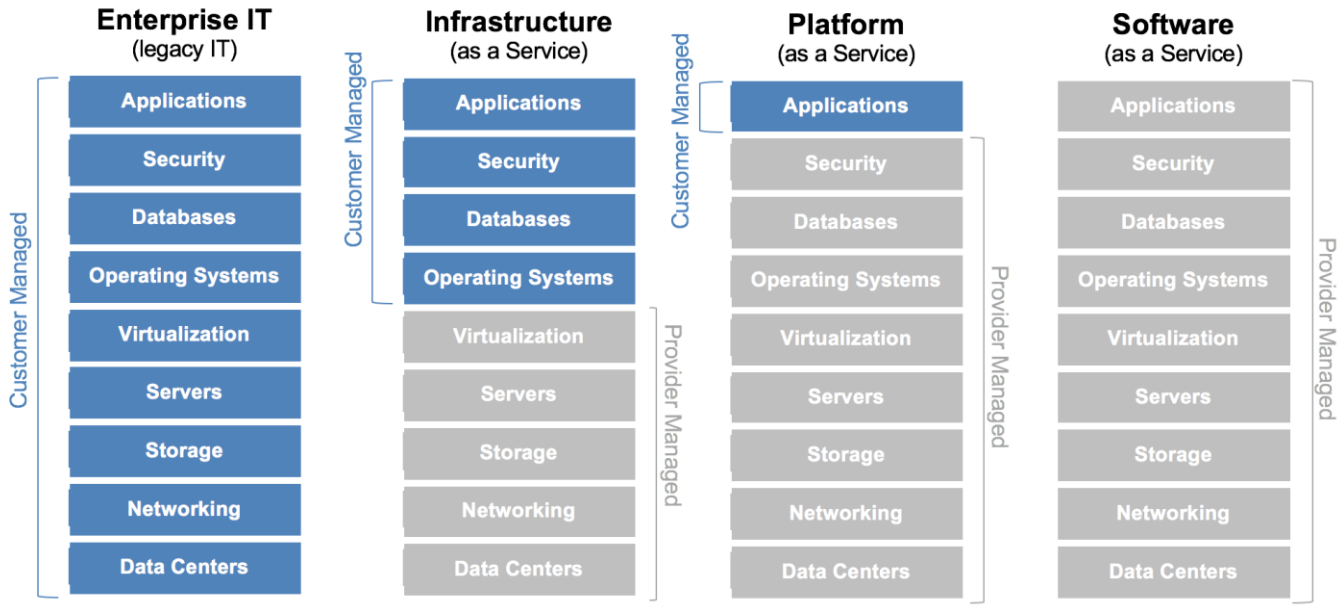
We exclusively use Microsoft cloud services and Accellion kiteworks environments for all high value workloads. Employees, consultants and contractors do not store or access data analytics workloads in any other environment. Wherever it is technologically achievable we use Platform as a Service (PaaS) or Software as a Service (SaaS) as this

maximises the components of the solution (technology stack) that the provider is responsible for, as outlined in Figure 1A. Our providers invest far more in information security than is possible for state government agencies. For example, Microsoft's cyber security budget exceeds USD$1B annually. Our strategy enables us to benefit from this investment.

We do not use Enterprise IT, for example on-premise infrastructure in server rooms, due to the unacceptable risks to information security that would result.

While there is no legislative restriction on storing or processing information overseas we maintain all high value workloads within Australia.

Figure 1A



Our information security framework

We implement the Victorian Protective Data Security Framework (VPDSF). We also use the Commonwealth's Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) to complement the VPDSF.

Consistent with the VPDSF and PSPF we focus on information security across the following domains:

- Security governance
- ICT security
- Information security
- Personnel security
- Physical security

Our controls

Certified controls

Our high value workload environments are certified or assessed as listed in Figure 2A.

Figure 2A

	Microsoft cloud services	Accellion kiteworks
FedRamp	✓	✓
SOC 2 Type 2	✓	✓
FIPS 140-2	✓	✓
HIPAA	✓	✓
GDPR	✓	✓
Australia Signals Directorate CCSL	✓	
ISO 27001:2013	✓	
NIST 800-53	✓	

As at April 2018, only five providers are certified by the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) to be on the Cloud Certified Services List (CCSL) for the storage, communication and processing of information with a PROTECTED classification.

Our Microsoft workloads are certified against approximately 60 additional regulations, rules, standards, programs, security control catalogues and other compliance requirements. An exhaustive list is at:

- https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

Additional controls

While our environment is primarily managed by Microsoft and Accellion we have strong governance and compliance oversight of the residual risks of this model and have additional configuration and security controls to address them. Those security controls focus on account breach, elevation of privilege, data exfiltration, data deletion, data spillage, malicious insider, phishing, whaling, spoofing, password cracking risks and malicious personnel risks.

ICT controls

- Multi factor authentication is enabled on all administration and user accounts
- We do not expire passwords and have password strength requirements consistent with NIST Special Publication 800-63-3
- We have alternative contact information for all users to safely contact users to verify anomalous activity
- We have adopted the Office 365 Advanced Security Management Console
- We have enabled the Office 365 Advanced Threat Protection Safe Attachments feature
- We have enabled the Office 365 Advanced Threat Protection Safe Links feature
- We have enabled the Office 365 customer lockbox feature, which requires Microsoft to get our approval for any operation that grants a Microsoft employee direct access to any information
- We have OS security updates and version monitoring
- We monitor Windows Defender Antivirus status on every end-user laptop
- We check to ensure that the following Windows Defender components have been configured to recommended baselines on every end-user laptop:
    - Exploit Guard
    - Application Guard

    - SmartScreen
    - Firewall
    - Credential Guard
- We monitor to ensure BitLocker has been configured properly according to recommended baselines on every end-user laptop on supported drives

Personnel controls

In accordance with our pre-employment screening policy, we require all personnel (including contractors) to:

- verify their identity
- undergo reference checks
- verify their highest tertiary qualification(s)
- verify any qualification(s) that are not a requirement of their position
- complete a National Police Check
- complete a thorough induction
- verify their work rights

We manage the ongoing suitability for employment of all personnel by requiring them to:

- complete a National Police Check every three years
- disclose any new charges and/or convictions
- make an annual attestation in relation to charges and convictions
- complete an annual Declaration of Independence

We also have a procedure for personnel to declare any conflicts of interest.

Information security controls

VAGO have assessed all our information assets and classified them considering the potential compromise to confidentiality, integrity and availability. We have developed an information management framework to establish, implement and maintain information security controls.

We ensure that only authorised people access information through approved processes, consistent with the Victorian Protective Data Security Standards (VPDSS) and Australian Auditing Standards, such as ASQC 1. This means that only the financial or performance audit engagement team, including data analytics personnel and information systems audit personnel assigned to an active audit, have access to your information.

Consultants are unable to access data analytics workloads unless approved by the Auditor-General.

Physical security controls

We maintain very low levels of paper material and our clear desk procedure mandates that this material is secured in locked drawers when not in use. It also mandates that computers are digitally locked when personnel are away from them and are physically locked away at night.

Visitors to our office are electronically registered and we have a permission driven swipe-card access control system in place.

Even though all end-user laptops have BitLocker installed, storage of data on them is discouraged for information hygiene reasons.

We do not allow the acquisition of data using USB sticks and USB ports are disabled on all devices to prevent this

Assessment and assurance

Microsoft cloud services

Independent third-party audits, compliance and assessment reports, authorisations, certificates and other compliance documents are at:

- https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide

Information on how Microsoft cloud services further manage information security including audit controls, FAQs, white papers, pen tests and security assessments are at:

- https://servicetrust.microsoft.com/ViewPage/TrustDocuments

Accellion kiteworks

FedRamp authorisation verification is at:

- https://marketplace.fedramp.gov/#/product/kiteworks-federal-cloud?sort=productName

FIPS 140-2 validation is at:

- https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3219

Additional compliance information is available at:

- https://www.accellion.com/platform/governance/file-sharing-governance

A security whitepaper and SOC 2 Type 2 report on controls is available on request and subject to entering an NDA with Accellion.

Additional controls

We ensure that our additional controls are operating as designed through our internal audit and other test programs. Our most recent tests are:

- External and Internal Penetration Test (November 2017)
- Social Engineering Testing (February 2018)
- Physical Penetration Test (June 2018)
- Physical Security Review (June 2018)
- Clean desk and secured laptop audits (May, June and July 2018)

Continuous monitoring

Microsoft cloud services

We actively monitor Microsoft's compliance posture against ISO 27001:2013 and NIST 800-53 using the Compliance Manager tool, which is at:

- https://servicetrust.microsoft.com/ComplianceManager

Access to the Compliance Manager is available to all clients on request.

Additional controls

We maintain compliance oversight of these and other controls using:

- https://securescore.office.com
- https://portal.cloudappsecurity.com
- https://securitycenter.windows.com
- Click Sense compliance dashboard
- Qualys

Reporting and executive sponsorship

The following items are reported weekly to the Operational Management Group in writing:

- Overdue National Police Checks
- Staff without a profile photo
- Overdue Declarations of Independence

The following are reported monthly to the Operational Management Group in writing:

- Additional configuration and security controls compliance
- Firewall threats
- Remote access users
- Unpatched systems
- Assets with un-patchable vulnerabilities
- Assets with easily exploitable vulnerabilities
- Active 0-day threats
- Hosts with active severity 5 and 5 vulnerabilities
- Assets with patchable and actively exploited severity 5 vulnerabilities

The following are reported monthly to the Chief Information Officer:

- Open ports overview
- Threat protection
- Visit to malicious URLs
- Blocked application activity
- Blocked user activity

Other non-compliance is reported to the Operational Management Group as encountered.

Our Security Projects Group is responsible for:

- a coordinated approach to our security
- compliance with the Victorian Protective Data Standards Framework
- developing controls to deliver on our risk appetite for no unauthorised disclosures or breaches of information security