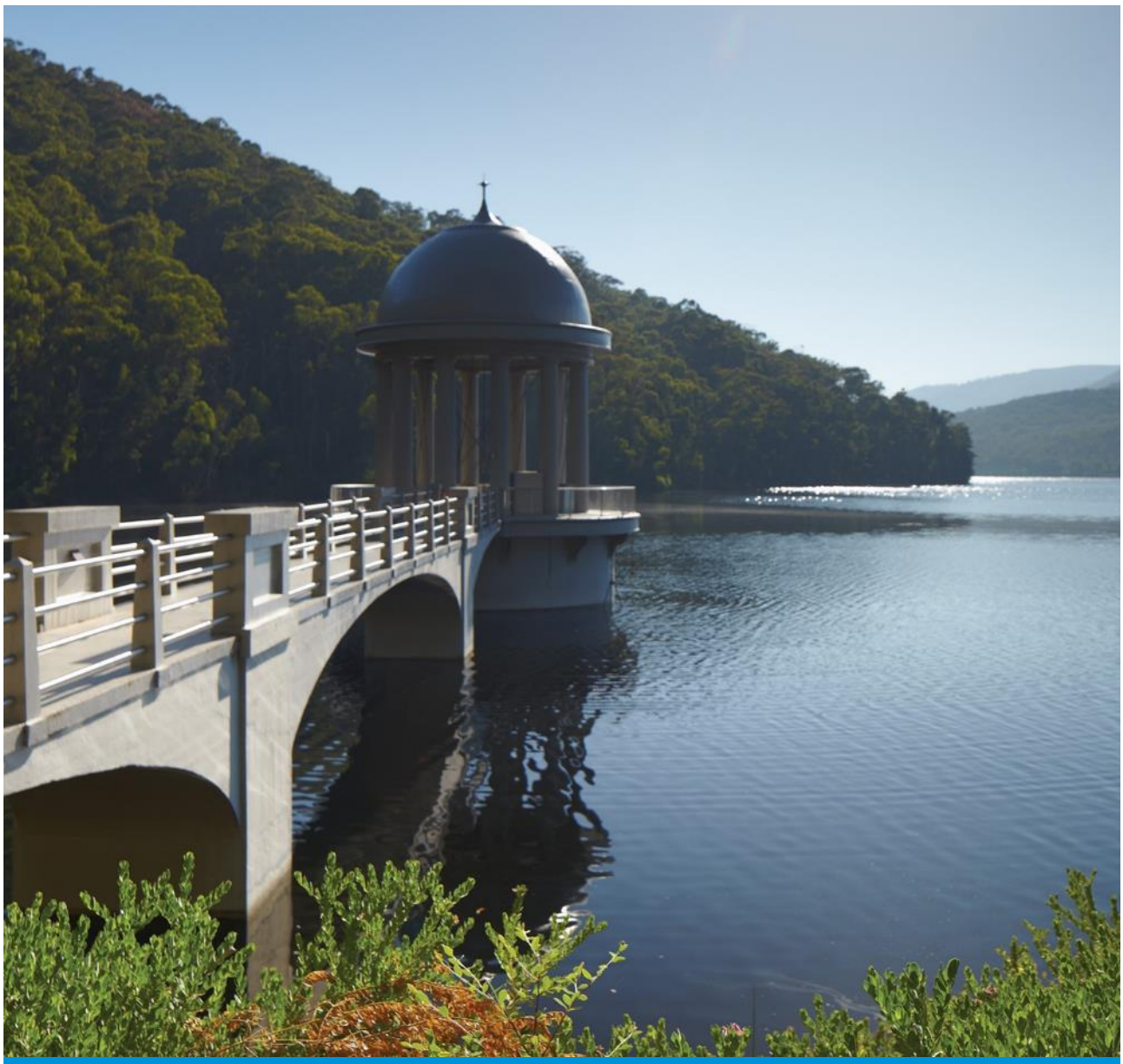

Supplier Security Standard

April 2025

Table of contents

1. Purpose 3
2. Scope 3
3. Exemptions 3
4. Definitions 3
5. All Suppliers 4
5.1 Information Security Management 4
5.2 Security Incident Response 4
6. Data Security 4
6.1 Data Security & Compliance 4
6.2 Data Handling & Protection 4
6.3 Data Sovereignty 5
6.4 Security Audits & Monitoring 5
6.5 Data Retention & Disposal 5
7. Network Security 6
7.1 Access Control & Least Privilege 6
7.2 Secure Remote & On-site Access 6
7.3 Endpoint Security & Device Compliance 7
7.4 Logging, Monitoring & Auditing 7
7.5 Offboarding & Access Termination 7
8. Document History 7

1. Purpose

This Supplier Security Standard defines security control objectives for Melbourne Water's third-party suppliers ("**Standard**").

The control objectives contained in this Standard ensure the safe, secure, and compliant delivery and operation of Melbourne Water's systems and services within its risk appetite and in compliance with its external obligations.

2. Scope

This Melbourne Water IT Security Standard applies to any third-party provider of services to Melbourne Water ("**Supplier**").

This Standard contains a base set of requirements, and additional controls may be required of the Supplier, applied through contractual arrangements and/or the provision of additional security requirements, policies or standards by Melbourne Water.

In the event any aspect of this Standard is inconsistent with a term of a contract made with a Supplier, the contract shall prevail to the extent of the inconsistency.

3. Exemptions

Any exemptions to the application of this Standard to a Supplier must be approved by Melbourne Water's Senior Manager, Technology Risk and Compliance and registered in an exemptions register, and any additional risk associated with each approved exemption must be approved by Melbourne Water in accordance with Melbourne Water's Risk Management Framework.

4. Definitions

Term	Definition
Melbourne Water Data	Information created, collected, processed, stored, or managed in the course of Melbourne Water operations.
Personal Information	Information or an opinion that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
Role-Based Access Control (RBAC)	Access control is based on user roles, which group permissions needed for specific organisational functions. Roles may inherit permissions through a hierarchy and can apply to one or multiple users.

In addition, the following terms are used throughout this Standard:

- "must", or the terms "required" or "shall", means that the statement is an absolute obligation placed on the responsible team or role.
- "should" or the adjective "recommended", means that there may exist valid reasons in particular circumstances to not fulfil this objective, but the full implications must be understood and carefully weighed before choosing a different course.

5. All Suppliers

5.1 Information Security Management

5.1.1 The Supplier must maintain a documented, management-approved information security policy that is regularly reviewed and communicated to relevant personnel.

5.1.2 The Supplier must promptly provide their information security policy to Melbourne Water upon request.

5.2 Security Incident Response

5.2.1 Suppliers must report any suspected or confirmed security incident, data breach, or unauthorised access to Melbourne Water within 24 hours of becoming aware of the breach.

5.2.2 In the event of a security breach, Melbourne Water reserves its right to:

- Revoke Supplier access immediately;
- Conduct a post-incident review; and
- Require the Supplier to promptly implement corrective security measures in Melbourne Water's absolute discretion.

5.2.3 The Supplier must fully cooperate with Melbourne Water regarding incident investigations, including forensic analysis, remedial actions, and the timely supply of supporting evidence.

6. Data Security

This section applies to third-party suppliers who create, collect, process, store, or manage Melbourne Water Data per Melbourne Water's requirement to comply with the Victorian Protective Data Security Standards (VPDSS) for public sector information and Australian legislation.

6.1 Data Security & Compliance

6.1.1 The Supplier must implement and maintain security controls that support compliance with the VPDSS and all applicable data security policies of Melbourne Water. The Supplier must ensure that any subcontractors, service providers, or affiliates engaged by the Supplier who handle Melbourne Water Data comply with equivalent security requirements to the VPDSS.

6.1.2 Personal information must be managed in accordance with Information Privacy Principles specified in the *Privacy and Data Protection Act 2014 (Vic)*.

6.2 Data Handling & Protection

6.2.1 The Supplier must protect Melbourne Water Data from unauthorised access, disclosure, modification, and loss.

6.2.2 Melbourne Water Data must be encrypted at rest and in transit using industry-standard cryptographic methods.

6.2.3 The Supplier must implement access controls based on the principles of least-privilege and need-to-know.

6.2.4 The Supplier must utilise secure email systems that are protected against unauthorised access and malicious content.

6.2.5 Personnel who require access to information classified as Protected under the *Security of Critical Infrastructure Act 2018* must understand restrictions on disclosure and comply with Melbourne Water information handling policies.

6.3 Data Sovereignty

6.3.1 The Supplier must store and process Melbourne Water Data only jurisdictions that are expressly approved by Melbourne Water.

6.3.2 Melbourne Water Data must not be transferred outside Australia without the prior written approval of Melbourne Water.

6.4 Security Audits & Monitoring

6.4.1 Melbourne Water reserves its right to conduct periodic security audits of the Supplier's systems and facilities.

6.4.2 The Supplier must promptly provide to Melbourne Water any relevant security assessment reports, including penetration testing and vulnerability scans, upon request.

6.4.3 The Supplier must rectify any security deficiencies impacting the confidentiality or integrity of Melbourne Water Data within 28 days of being identified.

6.5 Data Retention & Disposal

6.5.1 Upon contract expiry or termination or at any time directed by Melbourne Water, the Supplier must securely return, delete, or destroy all Melbourne Water Data, using industry-standard data sanitisation methods.

6.5.2 The Supplier must provide a certificate of destruction confirming that Melbourne Water Data has been securely disposed of.

6.5.3 Information must be managed and retained in accordance with the Public Records Office of Victoria Retention and Disposal Authorities (RDA).

7. Network Security

This section applies to all third-party suppliers, contractors, and external personnel who require network access to Melbourne Water systems, whether on-site or remote.

All Supplier staff and contractors who are provisioned a Melbourne Water user account must read and accept the Melbourne Water Acceptable Use Policy, and any activity on Melbourne Water systems must comply with the Melbourne Water Security Management Policy and Standards.

7.1 Access Control & Least Privilege

7.1.1 Supplier personnel access must follow the principle of least privilege, granting only the minimum necessary permissions required for an individual's role.

7.1.2 Supplier personnel must use individual, uniquely identifiable accounts. Shared accounts are not permitted.

7.1.3 Melbourne Water shall enforce Role-Based Access Controls (RBAC) and conduct periodic access reviews to remove unnecessary or inactive accounts.

7.1.4 Multi-factor authentication (MFA) is mandatory for all Supplier remote access to Melbourne Water systems.

7.1.5 Privileged access (for example, administrative or elevated permissions) must be time-limited and logged. Where possible, just-in-time (JIT) or temporary access should be used instead of persistent privileged accounts.

7.1.6 All Supplier access to the Melbourne Water network must be subject to automatic expiration upon contract completion, role changes, or inactivity beyond a defined period.

7.1.7 Any personnel who are required to access any critical infrastructure components of Melbourne Water under the *Security of Critical Infrastructure Act 2018* must be identified in Melbourne Water's SOCI compliance program.

7.2 Secure Remote & On-site Access

7.2.1 Supplier access to the Melbourne Water network must be segmented and/or restricted to only the systems required for an agreed scope of work.

7.2.2 Remote access must be conducted through secure, Melbourne Water-approved methods, such as:

- Virtual Private Network (VPN) with strong encryption
- Zero Trust Network Access (ZTNA) solutions
- Secure Remote Desktop environments

7.2.3 Melbourne Water may log and monitor all third-party network connections, including remote sessions, to detect anomalies and unauthorised access attempts.

7.3 Endpoint Security & Device Compliance

7.3.1 All devices used for Melbourne Water network access must meet Melbourne Water's security standards, including:

- Up-to-date operating system and security patches
- Endpoint Detection and Response (EDR/XDR) solutions enabled
- Disk encryption for data protection

7.3.2 Melbourne Water reserves its right to enforce security controls on supplier-managed devices, including network access restrictions, monitoring, and mandatory security configurations.

7.3.3 Devices that fail to meet Melbourne Water's security requirements may be blocked from connecting to Melbourne Water systems, in Melbourne Water's discretion, until compliance is achieved.

7.3.4 Personal devices must not be used to access the Melbourne Water's network unless expressly authorised and secured under Melbourne Water's endpoint management program.

7.4 Logging, Monitoring & Auditing

7.4.1 All Supplier access to the Melbourne Water network may be logged and retained in accordance with Melbourne Water security and compliance policies.

7.4.2 Logs may capture authentication attempts, privileged access, and data interactions, with regular reviews conducted by Melbourne Water's security team.

7.4.3 Melbourne Water may conduct regular access audits to verify Supplier compliance and remove any inappropriate access.

7.5 Offboarding & Access Termination

7.5.1 Supplier access to the Melbourne Water network may be immediately revoked upon by Melbourne Water:

- Completion of the contract or project;
- Staff departure, or role changes that no longer require access; or
- Detection of non-compliance with Melbourne Water's security policies.

7.5.2 Melbourne Water must ensure that all access credentials, tokens, and certificates issued to third-parties are deactivated and securely removed from systems.

8. Document History

Date	Reviewed/ Actioned By	Version	Action
April 2025	Melbourne Water Cybersecurity	3	Corrections made to document.

Date	Reviewed/ Actioned By	Version	Action
April 2025	Melbourne Water Cybersecurity	2	Corrections made to document.
March 2025	Melbourne Water Cybersecurity	1	