Information Security Policy

Last reviewed: 31/10/2024

Purpose and rationale

The purpose of this policy is to protect any data that is stored, accessed, transmitted, displayed, relayed and/or processed by WMQ people or systems. The protection of not only our own information, but the information we hold around people is very important to us. We do this by aligning our information security objectives to our strategic values.

Scope

This policy applies to the WMQ workforce, external service providers and other authorised users who access its information assets and associated information systems. All information created, presented and maintained by and/or output from WMQ's information systems is in scope. Throughout this policy, the term "information" is used to refer to any data, irrespective of its file format and how it is stored.

Requirements

What is information security?

Information security relates to the capabilities in place to protect company assets and information from a wide range of threats, to ensure business continuity, minimise business damage and maximise return on investment.

Information security principles

The three fundamental principles of Information Security are directed at the preservation of confidentiality, integrity and availability of the information. This policy is based on these principles.

- ***Confidentiality*** - information must be accessible only to those authorised to have access for an authorised purpose.
- ***Integrity*** - the accuracy and completeness of information and processes must be safeguarded. Information must not be changed without authorisation and should be sufficiently accurate for the purpose for which it is used at the time it is used.
- ***Availability*** - authorised users shall have access to information and associated assets as and when required.

Information security responsibility

Everyone who has access to WMQ information has a duty to use it responsibly and in accordance with the security policies. The information security requirements are designed to enable our workforce to work productively and securely. This practice will keep our workforce and WMQ safe from physical and cyber security threats. Everyone is expected to protect WMQ information both in written and verbal form, wherever it is stored and used including customer data, employee data and company data, as per WMQ's data classification. Executive Leadership Team shall be committed to work with the Information Security Team to establish, implement, operate, monitor, and ensure continuous improvement of ISMS.

The WMQ workforce is required to:

- Protect the information from unauthorised use or disclosure
- Protect the information from unauthorised modification and ensure it is accurate
- Ensure the information is available to authorised parties when required
- Complete periodic information security awareness training
- Comply with information security policies.

Exception to information security

Exceptions to all WMQ security policies and standards shall be received by the Service Desk Team and assessed by WMQ Information Security Team, recorded in the policy exception register and sent for endorsement by the General Manager, Technology & Operations and the Virtual Information & Digital Security Manager (VCISO), with approval by the Director of Organisational Transformation. All exceptions shall be discussed and approved during the Information Security Management System (ISMS) Forum.

More information

Information security policies, standards and related documents are available at Policy & Resource Library on WMQ intranet site (HUB). Please contact the information security team at infosec@wmq.org,au if you have any queries in relation to this policy.

Appendix A – Information Security Standards Summary

All staff are expected to understand and comply with the Information Security Policy and related standards. These are available on Policy and Resource Library

Standard	Purpose
Information System Acceptable Use Policy	This standard provides additional information on acceptable use of a variety of information assets, systems and devices, compliance activities and are enforceable.
Information Security Governance Standard	Sets out the principles, security controls and objectives for the handling, processing and storage of all information owned by or entrusted to the WMQ.
Identity and Access Management Standard	Describes types of digital identities in use for systems and applications; criteria for creating accounts and password requirements.
Data Classification, Retention and Disposal Standard	Describes the types of data, how to classify the data, data retention requirements as per classification and how to dispose of the data.
Security Logging Standard	Sets out the requirements for the logging and monitoring of system environments.
Network Security Standard	Sets out high-level security requirements for networks, wired, wireless, remote access, firewall, IDS/IPS, Cloud and other network related security.
Systems Development Security Standard	Sets out the requirements for security during the systems development process including initiation, analysis, design, build, testing, acceptance, deploying and maintenance.
Third-Party Security Standard	Sets out the security requirements for vendor access to Information Systems including engagement, technology enablement, monitoring, assurance and rolling-off.
Data Encryption and Key Management Standard	Sets out the requirements for data encryption, selection of industry best practices and how to manage the encryption keys.

Standard	Purpose
Endpoint Security Standard	Sets out the requirements for endpoint systems.
Vulnerability and Patch Management Standard	Describes how to identify the vulnerability in WMQ systems and network, how to categorize these and how to patch them under patch processes.