CYBER SECURITY POLICY

1. Overview

1.1 Policy at a glance

This policy provides management direction and support for cyber security across Hunter Water.

1.2 Scope

The Cyber Security Policy applies to all our people (as defined).

The policy applies to all interactions with Hunter Water's digital infrastructure and/or access to Hunter Water's systems, applications and information.

The resources included in the scope of this Cyber Security policy are:

- Information, data and digital assets created and managed by Hunter Water, including outsourced information, data and digital assets;
- Information and communications technology (ICT) systems which process information; and
- Communication networks which transport information including the Operational Technology (SCADA) networks, associated infrastructure and Internet of Things (IOT) devices that handle Hunter Water or third party data or provide critical Hunter Water services.

2. Policy statement

This policy aligns with the Corporate value of trust. Hunter Water believes that stakeholder trust can be maintained and enhanced through the development of a security culture and an associated technical capability to identify and respond to information security incidents in a timely manner. The security of our information is critical to ensuring the resilience and ongoing success of Hunter Water. Hence, it is the policy of Hunter Water that the information it manages shall be appropriately secured to ensure:

- Confidentiality of information is maintained preventing disclosure of sensitive business or personal information to unauthorised persons through deliberate or unintentional action;
- Integrity of information is maintained by prevention of unauthorised modifications;
- Information is only available to authorised users when needed;
- Information security training is provided to all our people who interact with our systems;
- All breaches of information security and suspected weaknesses are reported and investigated; and
- Information security practices at Hunter Water are aligned with the NSW Cyber Security Policy 2019, and with the ISO/IEC 27001:2013 Information Security Management Standard (ISMS).

Cyber Security Objectives

The information security objectives of Hunter Water's ISMS are:

- Maintain the reputation and brand of Hunter Water;
- Ensure Hunter Water complies with all applicable external regulatory requirements;

- Ensure the integrity and availability of critical business applications to meet operational needs;
- Develop a culture that sees information security embedded in decision making; and
- Continuously improve the security posture of Hunter Water through the management of risks, threats and incidents whilst balancing the utility and protection of information.

3. Application of policy

All our people commit to the following:

1.	Agree to, understand and exhibit the requirements of the Acceptable Use of Electronic Resources Standard.
2.	Agree to, understand and exhibit the requirements of the Code of Conduct. Of particular relevance for this policy are the requirements around confidentiality, privacy, intellectual property and use of Corporate assets.
3.	Comply with all requirements surrounding passwords and access to Corporate systems including Bring Your Own Device (BYOD) and remote access or elevated privileges.
4.	Be vigilant when using email and internet services to validate attachments or links before opening or clicking them.
5.	Report suspicious emails to the Cybersafe reporting email address for investigation.
6.	Report actual or suspected cyber security incidents to your immediate supervisor and/or Service Desk.

In addition to the above, Hunter Water directors, executives, managers and team leaders will:

1.	Facilitate and support a culture where cyber security is considered throughout our business processes and decision making.
2.	Ensure that they, and those within their area of responsibility, are aware of, understand and comply with the requirements of the Acceptable Use of Electronic Resources Standard and Code of Conduct at all times.
3.	Ensure that any new business systems or applications are procured or developed in conjunction with the Digital team from an early stage to ensure that proper consideration can be given to the cyber security requirements of these systems.
4.	Actively support our people in reporting actual or suspected cyber security breaches and assist with any questions or concerns people have about cyber security or the requirements of the ISMS.
5.	Take the appropriate action as outlined in the relevant ISMS standards and procedures if they become aware or actual or suspected breaches of cyber security

Failure to comply with any element of this policy may result in disciplinary action, up to and including termination of employment in accordance with Hunter Water Corporation's Code of Conduct, and the Misconduct and Discipline Standard. Each situation will be treated individually on a case-by-case basis.

4. Associated regulations and standards

Interaction with other ISMS Standards and procedures

Document Type	Title
Standard	Acceptable Use of Electronic Resources Standard
Standard	Information Security Standard
Standard	Access Management Standard
Standard	Remote Access Standard
Standard	Mobile Device Standard
Standard	Information Classification and Handling Standard
Standard	Asset Management & Disposal Standard
Standard	Operational Security Standard
Standard	Communications Security Standard
Standard	Cryptographic Security Standard
Standard	Systems Acquisition and Development Standard
Standard	Supplier Management Standard (Digital)
Procedure	Access Management Procedure
Procedure	Digital Change Management Procedure
Procedure	Information Security Incident Management Procedure

Other relevant documents

Document Type	Title
Policy	Code of Conduct
Policy	Risk Management
Standard	Misconduct and Discipline
Plan	Hunter Water Strategic Business Plan
Plan	Hunter Water Information Security Strategy

ASSOCIATED LEGISLATION, REGULATIONS & STANDARDS (External)

Document Type	Title
Act	Privacy and Personal Information Protection Act 1988 (NSW)
Act	Privacy Act 1988 (Cth) (including Notifiable Data Breach Scheme)
Act	Health Records and Information Privacy Act 2002 (NSW)
Act	Government Information (Public Access) Act 2009 (NSW)
Act	Security of Critical Infrastructure Act 2018 (Cth)
Policy	Cyber Security Policy 2021 (NSW)

5. Definitions, acronyms and abbreviations

Term	Definition
Cyber Security	Cyber Security refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction or inspection by those unauthorised to do so. It also considers the threats posed by physical access to information by physical attendance at corporate premises.
ISMS	Information Security Management System
People	For the purposes of this Policy, this includes: • directors • permanent employees, whether full-time or part-time • temporary or casual employees • consultants • individual contractors working for or on behalf of Hunter Water • employees of contractors providing services to Hunter Water • volunteers, secondees, work experience students.

Signed: 

Darren Cleary
Managing Director

Approved by:	Managing Director	Approved date:	09/05/2022
Maintained by:	Security Audit & Compliance Officer	Next scheduled review date:	09/05/2027
TRIM File No.	HW 2015-525/2.005	Version:	2.0