PURPOSE

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

Specific, subsidiary information security policies and standards shall be considered part of this information security policy and shall have equal standing.

SCOPE

This policy applies to all Hunter Water employees, contract and casual staff and third parties. This includes permanent, temporary and casual staff of Hunter Water, staff seconded from other organisations, and contingent workers including labour hire, professional services contractors and consultants, who may utilise Hunter Water's infrastructure and/or access Hunter Water's systems, applications and information.

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

- Information in any medium or form such as printed paper, digital, video, and audio representations;
- Information systems which process information; and
- Communication networks which transport information.

POLICY STATEMENT

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 by prevention of disclosure to unauthorised persons through deliberate or unintentional action;
- Integrity of information is maintained by prevention of unauthorised modification;
- Information is available to authorised users when needed;
- Information security training is given to all employees; and
- All breaches of information security and suspected weaknesses are reported to the ICT Service Desk and investigated.

Information security practices at Hunter Water comply with the NSW Government Digital Information Security Policy, and are aligned with the ISO/IEC 27001:2013 Information Security Management Standard.

SECURITY OBJECTIVES

This policy supports the following security objectives of Hunter Water:

- Ensure customer data is protected in accordance with any legal and statutory obligations;
- Continuously improve the security posture of Hunter Water;

- Ensure critical business applications are available when required;
- Establish a consistent approach to the assessment, management and treatment of information security risks within the scope of the ISMS;
- Management of internal and external threats including gap analysis and treatment plans to address the risks posed by such threats;
- Report and investigate all information security incidents and suspected weaknesses, and resolve in accordance with the assessed risk; and
- Maintain the reputation and brand of Hunter Water.

NON-COMPLIANCE AND DISCIPLINARY ACTIONS

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 Disciplinary Standard. Each situation will be treated individually on a case-by-case basis.

POLICY ADMINISTRATION

Effective from	1 December 2017
Approved by	Managing Director
Policy Owner	Chief Information Technology Officer
Policy Administrator	ICT Security, Audit and Compliance Officer
Application	This policy applies to all persons working in or for Hunter Water, including contractors and consultants.
Last review date	20 November 2017
Next review date	20 November 2020
Version	1.2
File reference	HW2015-525/2.005
Published externally	No
Approval Signature	 **Managing Director / ~~Company Secretary~~**

RELATED DOCUMENTS

- Information Security Standards and procedures

ASSOCIATED REGULATIONS AND STANDARDS

- NSW Government Information Classification, Labelling and Handling Guidelines
- Information Security Management System ISO/IEC 27001:2013
- Privacy and Personal Information Protection Act 1998 (PPIP Act)
- Digital+ 2016 NSW Government ICT Strategy