Yorkshire Water Information Security Policy

(Part of the Information Security Policy Framework)

Related Group Area & Processes: Information Security

Document Originator: [redacted]

Document Status: Live

Document Authorised By: Information Security Forum

Document Approved By: Security Steering Group

Control areas(s): ISMS: 5.2, A. 5.1.1

1. Contents

2. Purpose, Scope and Objectives

Information is an asset, and like any other business asset it has value and must be protected. This value is not just financial but is based on the impact on individuals and the company, should this information be compromised in any way. This document sets out policy on Information Systems Security across Yorkshire Water.

This Policy is part of the Information Security Policy Framework and is supported by, and should be applied in conjunction with, specific individual Information Security Policies and Procedure documents which are available via Yorkshire Water intranet sites.

In order to ensure the Confidentiality, Integrity and Availability of the Company's information and to meet its legal, regulatory and contractual obligations, the Company has implemented an Information Security Management System ('ISMS'). This system has the support and approval of the Board of Directors. The Information Security Team are responsible for the management, running and continual improvement of an ISMS to meet the requirements of the information security standard ISO/IEC 27001:2013 ('the Standard').

To help achieve continual improvement of managing Information Security, Yorkshire Water has a process to help track and manage operational and security control objectives. The security controls and policies will be measured for effectiveness and achievement of intended outcomes as determined by 'the Standard'.

This policy applies to all:

1. Personnel/ Users (including Yorkshire Water employees and contracted third parties operating on behalf of Yorkshire Water).
2. Company owned and managed IT Equipment, communications systems (including network communications, email, Internet and Guest wireless network access) and information management systems and services.
3. Company owned data and information
4. Use of company equipment, software and information.
5. Logical, Physical and home working environments

The objective of this policy is to;

1. Safeguard all information systems assets against compromise resulting from cyber-attack, misuse, abuse or failure whether through accidental or deliberate means
2. Ensure the pseudonymisation (rendering unidentifiable) and encryption of personal data
3. Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
4. Ensure we can restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
5. Maintain a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing (especially personal data collection, storage and transfer)

3. Definitions

The Information Security Policy is set out below. All references in the Policy to "the Company" means Yorkshire Water and any of its subsidiaries or associated companies.

"GDPR" refers to General Data Protection Regulation.

4. Policy

4.1 Information security and the protection of data will be achieved through compliance with the Yorkshire Water Information Security Policies
4.2 All Information Security Policies, Standards, Procedures and Guidance will be made available to Yorkshire Water personnel via an approved and communal platform
4.3 Systems storing and processing personal data must be protected using an appropriate balance of physical, procedural, personnel and technical controls to meet the requirements of the GDPR Article 32: Security of processing
4.4 The Company's information and information systems are provided to fulfil the legitimate business needs of the Company and must only be used for lawful purposes.
4.5 The Company views any misuse of its information or information systems very seriously, has the capability, and reserves the right to access, monitor, use, copy and delete any electronic information, data or e-mail messages to ensure compliance with this policy
4.6 The Company owns the copyright for all software (code, programs, systems), produced by an employee, agent or sub-contractor as part of their normal duties or terms of employment or contract.
4.7 All collection, storage, processing and use (including monitoring) of personal data must be registered by the Data Controller of the Yorkshire Water in accordance with the requirements of the General Data Protection Regulation (GDPR)
4.8 Deliberate, unauthorised entry to systems, entry of false data and unauthorised changes to systems and software are strictly forbidden and may constitute an infringement of the Computer Misuse Act
4.9 Software must not be copied. Unlicensed software must not be loaded or run on the Company's Equipment & Systems; this is illegal and is an offence under the Copyright, Designs and Patents Act
4.10 All Company information (both digital and printed) should be classified and handled in line with the **Kelda Group Information Security Classification and Handling Policy**
4.11 All users of the Company's information and information systems are personally responsible for any failure to comply with computer and Information related legislation.
4.12 Existing or newly identified information security risks will be regularly reviewed in order to prevent a compromise of confidentiality, integrity or availability of information assets. Risk treatment will take place for any risks that rise above the company's risk appetite
4.13 The Business and IT continuity plans will be continually developed and tested on a regular basis by designated areas of the Business.
4.14 Information Security Considerations will be contained within the recovery plans and activities.

5. Roles and Responsibilities

Information Security Manager
Oversee the ongoing management of the ISMS ensuring it continues to meet business operational needs. Ensure that policies and procedures related to Information Security are established, documented, communicated and distributed where necessary within the Yorkshire Water.

Information Security Team
Are authorised to enforce this Information Security Policy Framework and will publish updated versions of this document based upon any related business changes or changes to the risk environment relating to information security.

Information Security Forum
Has the delegated authority for ensuring Information Security Governance, Policy, Risk, Compliance, Training and Awareness are managed effectively. The authority to approve supporting Information Security standards, guidance and procedures has been delegated to the Security Forum.

Security Steering Group
Will manage changes to and document its approach to meet any identified contractual, legislative or regulatory information security related requirements. They will continually improve and resource the ISMS to meet the Yorkshire Water's contractual, regulatory and legislative information security requirements and track security compliance. Final approve of the Information Security Policy Framework and sign off hierarchy is achieved at this level.

Individual Responsibilities
All users of the Company's information and information systems are personally responsible for any failure to comply with computer and Information related legislation. This includes, but is not limited to, the 'GDPR', 'Computer Misuse Act' and the 'Copyright, Designs and Patents Act'. Guidance on this legislation can be obtained from the Legal Department.

6. Governance

- The Information Security Team will publish updated versions of this document based upon any related business/ regulatory changes, government advice or changes to the risk environment relating to information security
- The following changes can be made to this policy without prior authorisation from the Security Steering Group:
  - Section 7 – Supporting Standards & Processes
  - Control areas(s): ISMS:
- Breach of this policy could lead to formal action under the Yorkshire Water Conduct Policy
- Breach by any sub-contractor or agent of the Company may lead to termination of contract
- The business risk owner should seek support from the Information Security Team and other relevant departments where a collaboration on the risk is required
- Exemptions to this Policy may be granted in line with the Yorkshire Water Dispensation Policy

7. Supporting Standards & Processes

Supporting Policies

Yorkshire Water Security Policy
Yorkshire Water Acceptable Use Policy
Yorkshire Water Access Control Policy
Yorkshire Water Clear Desk & Screen Policy
Yorkshire Water Dispensation Policy
Yorkshire Water Classification & Handling Policy
Yorkshire Water Personnel Security Policy
Yorkshire Water Supplier Relationship Policy
Yorkshire Water Security Incident Management Policy

Supporting Standards

Yorkshire Water Hardware Standard
Yorkshire Water Software Standard
Yorkshire Water Use of Information Standard
Yorkshire Water Physical Security Standard
Yorkshire Water Mobile Device Standard
Yorkshire Water Information & Systems Access Controls Standard
Yorkshire Water Password Management Standard
Yorkshire Water Payment Card Data Standard
Yorkshire Water Privileged System & Service Account Access Control Standard
Yorkshire Water Classification Standard
Yorkshire Water Handling Standard
Yorkshire Water Personnel Security Standard
Yorkshire Water Supplier Relationship Standard
Yorkshire Water Security Incident Management Standard
Yorkshire Water Security Risk Management Standard

Supporting Processes

Yorkshire Water Classification & Handling Guidance
Yorkshire Water Security Decisions Governance
Yorkshire Water Incident Management Procedures (Playbooks)
Yorkshire Water Security Risk Management Governance

8. Version Control

Version	Date	Change	Change Description
2.0	22/07/2014	[redacted]	Initial Document Draft
3.0	22/09/2014	[redacted]	PCI V3.0 requirements added, reference to the new compliance tracker added, A/V control updated and the ISM's policy and procedure's responsibility for communication and establishment.

3.1	11/2/2015	[redacted]	Amended to meet Data Classification Policy, reorganize Policy area and sign off by [redacted].
3.2	2/6/2015	[redacted]	Amended following a review by [redacted]
3.3	29/7/2015	[redacted]	Amended Breach information following review by HR and comments from Legal
3.4	23/9/2015	[redacted]	Amended document format to meet standards
3.5	15/10/2015	[redacted]	Added in the roles reference to the PCI environment. Last Review.
4.0	7/4/2018	[redacted]	Typo amendment. Include (the Standard) as a reference to ISO27001 for clarity. Updated the mailbox link Updated GDPR section Reworded risk section for easier reading. Amended to include GDPR improvements on advice by external contractors. Approved by Security Steering Group June 2018
5.0	17/12/2018	[redacted]	Edited all Policy links
6.0	04/04/2019	[redacted]	Reformatted to meet standardised policy template. Removed duplications including clauses covered in the Information Security Standard Documents Added supporting polices, standards and guidance list Amended Kelda Group to Yorkshire Water

Review Period & Method: Reviewed annually or due to environment changes by the Security Forum. Change requires sign off by Security Steering Group