REMONDIS®
WORKING FOR THE FUTURE

INFORMATION SECURITY MANAGEMENT POLICY

REMONDIS JBT Ltd.
Stephenson Way
Barrington Industrial Estate
Bedlington
Northumberland
NE22 7DL

T 01670 827820
E info@remondis.co.uk
W www.remondis-jbt.com

Next Review: January 2020

THE COMPANY

REMONDIS JBT operates from two sites in the North East of England, our head office in Bedlington, Northumberland and our secondary site in Birtley, County Durham. Customers cover a range of business sectors throughout the North East of England, including industrial and commercial businesses, local authorities as well as small businesses and households. REMONDIS JBT manage waste streams including industrial and commercial and construction and demolition waste, in addition to the accepting of WEEE directive.

REMONDIS JBT operates established quality, environmental and health and safety policies and is accredited to ISO 9001, ISO 14001 AND BS OHSAS 18001. These standards are incorporated into an Integrated Management System, which sets out operating procedures and standards that the business follows. REMONDIS JBT is committed to achieving standards of excellence and continuous improvement in the operation of its site.

PURPOSE

The purpose of this Information Security Example Policy is to provide exemplar guidance in line with best practice for the production of an Information Security Policy appropriate for REMONDIS JBT.

SCOPE

The production of an Information Security Policy for systems, devices or applications and information deployed in support of REMONDIS JBT business functions.

APPLICABILITY

This Policy is applicable to and designed for use by any company that use or have access to REMONDIS corporate systems and/or information at any level.

TERMINOLOGY

Term	***Meaning/Application***
SHALL	*This term is used to state a **Mandatory** requirement of this Policy*
SHOULD	*This term is used to state a **Recommended** requirement of this Policy*
MAY	*This term is used to state an **Optional** requirement*

POLICY

The Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of REMONDIS JBT information. It is the overarching Policy for information security and supported by specific technical security, operational security and security management policies. It supports the 10 data security standards. This Policy covers:

- Information Security Principles.
- Governance – outlining the roles and responsibilities.
- Supporting specific information security policies – Technical Security, Operational Security and Security Management.
- Compliance Requirements.

INFORMATION SECURITY PRINCIPLES

The core information security principles are to protect the following information/data asset properties:

- Confidentiality (C) – protect information/data from breaches, unauthorised disclosures, loss of or unauthorised viewing.
- Integrity (I) – retain the integrity of the information/data by not allowing it to be modified.
- Availability (A) – maintain the availability of the information/data by protecting it from disruption and denial of service attacks.

In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A properties are breached. The aggregation effect, by association or volume of data, can also impact upon the Confidentiality property.

For REMONDIS JBT, the core principles are impacted, and the effect aggregated, when any data breach relates to customer data.

GOVERNANCE – ROLES AND RESPONSIBILITIES

All Staff

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting REMONDIS JBT business. All staff are responsible for information security and remain accountable for their actions in relation to REMONDIS JBT and customer information and information systems. Staff **shall** ensure that they understand their role and responsibilities, and that failure to comply with this Policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is accountable for information risk within REMONDIS JBT and advises the Board on the effectiveness of information risk management across the organisation. Operational responsibility for Information Security **shall** be delegated by the SIRO to the REMONDIS JBT Information Security Officer.

All Information Security risks **shall** be managed in accordance with the REMONDIS JBT Risk Management Policy.

Chief Information Security Officer

The Chief Information Security Officer is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes. The Information Security Officer **shall**:

- Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.
- Provide a central point of contact for information security.
- Ensure the operational effectiveness of security controls and processes.
- Monitor and co-ordinate the operation of the Information Security Management System.
- Be accountable to the SIRO and other bodies for Information Security across REMONDIS JBT.
- Monitor potential and actual security breaches with appropriate expert security resource.

Data Protection Officer

The Data Protection Officer is responsible for ensuring that REMONDIS JBT and its constituent business areas remain compliant at all times with Data Protection, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. The Data Protection Officer **shall**:

- Lead on the provision of expert advice to the organisation on all matters concerning the Data Protection Act, compliance, best practice and setting and maintaining standards.
- Provide a central point of contact for the Act both internally and with external stakeholders (including the Office of the Information Commissioner).
- Communicate and promote awareness of the Act across the REMONDIS JBT.
- Lead on matters concerning an individual's right to access information held by REMONDIS JBT and the transparency agenda.

Information Asset Owners

The Information Asset Owners (IAOs) are senior/responsible individuals involved in running the business area and **shall** be responsible for:

- Understanding what information is held.
- Knowing what is added and what is removed.
- Understanding how information is moved.
- Knowing who has access and why.

Senior Responsible Owners

All Senior Managers, Heads of Department, Information Risk Owners and Directors, defined as Senior Responsible Owners (SROs), are individually responsible for ensuring that this Policy and information security principles **shall** be implemented, managed and maintained in their business area. This includes:

- Appointment of Information Asset Owners (IAO) to be responsible for Information Assets in their area(s) of responsibility.
- Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks
- Supporting personal accountability of users within the business area(s) for Information Security
- Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries of this Policy and associated policies and procedures.

SUPPORTING PRINCIPLES

The Information Security Policy is developed as a pinnacle document which has further policies, standards and guides which enforce and support the Policy. The supporting policies are grouped into three areas: Technical Security, Operational Security and Security Management and are shown in the diagram overleaf. The Information Security Policy is closely aligned to REMONDIS JBT's Data Privacy Policy and relies upon, and supports, REMONDIS JBT's Security policies.

TECHNICAL SECURITY

The technical security policies detail and explain how information security is to be implemented. These policies cover the security methodologies and approaches for elements such as: network security, patching, protective monitoring, secure configuration and legacy IT hardware and software.

OPERATIONAL SECURITY

The operational security policies detail how the security requirements are to be achieved. These policies explain how security practices are to be achieved for matters such as: data handling, mobile & remote working, disaster recovery and use of social media.

SECURITY MANAGEMENT

The security management practices detail how the security requirements are to be managed and checked. These policies describe how information security is to be managed and assured for processes such as: information security incident response, asset management and auditing.

LEGISLATION

REMONDIS JBT is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation **shall** be devolved to employees and agents of REMONDIS JBT, who **may** be held personally accountable for any breaches of information security for which they **may** be held responsible. REMONDIS JBT **shall** comply with all relevant legislation appropriate; this includes but is not limited to:

- Data Protection Act 2018
- General Data Protection Regulation 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990

AUDIT

Audit will be performed as part of the ongoing REMONDIS JBT Audit Programme and the Information Security Officer **shall** ensure appropriate evidence and records are provided to support these activities at least on an annual basis.

REVIEW

This Policy **shall** be reviewed at least annually by the reviewers noted within the Reviewers section of this Policy. The Information Security Officer **shall** be responsible for ensuring the review is conducted in good order and follows due process for approval. The Information Security Officer is accountable for providing the results of ongoing reviews of information security implementation across REMONDIS JBT.

KEY WORDS

Information Security, Governance, Confidentiality, Integrity, Availability, Senior Information Risk Owner, Senior Risk Owner, Information Asset Owner, Information Security Officer, Data Protection Officer