# Information Security Policy

## Introduction

Riello UPS UK Limited and Riello UPS Ireland Limited provides essential service functions which rely on resources and business processes. The use of information assets must be in line with good professional working practices and procedures as well as statutory, regulatory and contractual requirements and must ensure the confidentiality, integrity and availability of all our information assets.

Information is an extremely important asset and enables Riello UPS UK Limited and Riello UPS Ireland Limited  to fulfil its business functions and obligations to our customers and suppliers and intent to implement and maintain ISO/IEC 27001. The international security standard for information security management systems provides mandatory requirements for implementing, reviewing and continuously improving an Information Security Management System (ISMS). The ISMS shall ensure Riello UPS UK Limited and Riello UPS Ireland Limited meets its statutory, regulatory and contractual information security requirements including those provided by the current General Data Protection Regulation (GDPR). Further to this, some of Riello UPS UK Limited and Riello UPS Ireland Limited ’s customers are only willing to deal with other companies which adhere to high information security standards and this increasingly means achieving and maintaining ISO 27001 compliance.

## Purpose

This policy defines the ISMS policy in terms of the characteristics of the business, the organisation and its assets. It establishes Riello UPS UK Limited and Riello UPS Ireland Limited’s principles, ambitions and objectives when utilising a management system for information security.

## Scope

The scope of this policy extends to all Riello UPS’s departments and employees, site visitors who use/access Riello UPS UK Limited and Riello UPS Ireland Limited 's information assets and any third-party subcontractors working on behalf of, or supplying service to Riello UPS UK Limited and Riello UPS Ireland Limited.

The Riello UPS UK Limited and Riello UPS Ireland Limited Scope Statement: -

***"The design, assembly, distribution and service of uninterruptable power systems (UPS)”***

The Riello UPS UK Limited and Riello UPS Ireland Limited objectives are to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

## Policy statement

Riello UPS UK Limited and Riello UPS Ireland Limited holds and protects a limited amount of data relating to customers, suppliers and employee information. The ISMS implement information security systems that protect this information**.**

The Information Security Management team, incorporating senior managers from various departments, is charged with the management and approval functions associated with the ISMS.

Riello UPS UK Limited and Riello UPS Ireland Limited are charged with establishing and continually improving the ISMS.

Riello UPS UK Limited and Riello UPS Ireland Limited will provide the framework for setting objectives and establish an overall sense of direction of principles for action with regard to security.

The ISMS will comply with applicable business and legal or regulatory requirements and contractual security obligations.

The approach to information security will be based on risk, as per the ISO 27001 standard and best practice.

The ISMS procedures will establish risk evaluation criteria that are aligned with the current Riello UPS UK Limited and Riello UPS Ireland Limited approved risk management procedures and policies.

The ISMS will be included into the current Integrated Management System (IMS).

The creation of the ISMS will include listing all information assets and the security risks that may arise for each. The resultant information will inform the IT and Compliance Director of prospective mitigation priorities.

The IT and Compliance Director will periodically review Riello UPS UK Limited and Riello UPS Ireland Limited ‘s current practices, policies and guidance to recommend any changes or improvements to ensure we apply appropriate security measures.

**Reference documents**

- ISO/IEC 27001 standard, clauses 5.2 and 5.3
- Risk Assessment and Risk Treatment Methodology
- Statement of Applicability
- List of Legal, Regulatory and Contractual Obligations (LUS)
- Data Breach Response and Notification Procedure

**Objectives and measurement**

**Information security controls**

The process of selecting the controls (safeguards) is defined in the Risk Assessment and Risk Treatment Methodology.

The selected controls and their implementation status are listed in the Statement of Applicability.

**Responsibilities**

Responsibilities for the ISMS are the following:

- The Managing Director is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available.
- The IT and Compliance Director is responsible for operational coordination of the ISMS and personal data protection as well as for reporting about the performance of the ISMS.

- The management team must review the ISMS at least once a year or each time a significant change occurs and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy and effectiveness of the ISMS.
- The Compliance Manager will implement information security training and awareness programs for employees.
- The protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset.
- All data breaches, security incidents or weaknesses must be reported to a manager and /or the Sales and IT manager.
- The Managing Director will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when.
- The Compliance Manager is responsible for adopting and implementing training, which applies to all persons who have a role in information security management.

This Policy has been approved and authorised by:

**Name:** Leo Craig

**Position:** Managing Director

**Date:** 05th February 2026

**Signature:**