RIDGE

INFORMATION SECURITY POLICY

CONTENTS

1. DOCUMENT CONTROL

1.1.   Distribution

This document, once issued, becomes a live document and, subject to updates and changes, shall be maintained as a configuration-controlled item. Any subsequent amendments must be submitted to the Systems Manager and controlled using document versioning.

DISTRIBUTION

1.2.   Version Control

VERSION	DATE	DESCRIPTION	CREATED BY	REVIEWED BY
1.0	23.09.2021	Initial Daft	LS	DW
1.1	25.11.2021	Initial Release	LS	DW
1.2	24.01.2022	Review	LE	DW

1.3.   Applicable Documents

DOCUMENT TITLE	DOCUMENT LOCATION
Information Security Domain Policy	Workspace
Information Security Incident Response Policy	Workspace
Risk Management Framework Policy	Workspace
Acceptable Use Policy	Workspace
Clear Desk and Clear Screen Policy	Workspace
Information Classification and Handling Policy	Workspace
Information Security Management Planning Procedure	Workspace
Disciplinary Procedure	Workspace

1.4.   Definitions and Abbreviations

ACRONYM	DEFINITION

2. POLICY STATEMENT

Ridge and Partners LLP (Ridge) takes information security very seriously and protecting our information and IT systems remains a top priority. The significance of not securing our information could expose our businesses and our clients to serious and damaging lasting affects; of which could threaten our reputation and ability to operate.

Our people, clients and regulators expect us to secure our information, in line with industry recognised practice. Equally, personal and client information is legally protected and requires close attention.

Ridge operates an Information Security Management System, aligned to the requirements of the International Standard ISO 27001; recognised as best industry practice in information security management. The Management System has been designed to support the achievement of our strategic business objectives, through effective application of information governance and risk management.

It is Ridge's policy to ensure that information is protected against the loss of:

▪ Confidentiality – information is only accessible to authorised Individuals.
▪ Integrity – the accuracy and completeness of information is Maintained.
▪ Availability – information is accessible to authorised users and processes when required.

The achievement of this policy requires everyone at Ridge to take great care when handling our information, and to know and act upon our individual and collective security responsibilities.

Ridge commits to the continual improvement of its information security management system.

Endorsement

25.11.2021

3. INFORMATION SECURITY MANAGEMENT SYSTEM FRAMEWORK

Ridge's Information Security Management System (ISMS) framework is structured and organised hierarchically to reflect the strategic, tactical, and operational requirements, necessary to continuously operate an effective security posture. Figure 1 illustrates the ISMS framework hierarchy.

Figure 1. ISMS Framework Hierarchy

The Information Security Policy defines the direction and governance arrangements of the ISMS, supported by system related security policies and operating procedures.

The ISMS framework will be formally approved and communicated to colleagues, and to third parties, as and when necessary.

Whilst most of the supporting policies and procedures are specific to those who hold security responsibilities; crucially every employee has a personal responsibility to read and understand the:

- Information Security Policy
- Acceptable Use policy
- Clear Desk and Clear Screen Policy
- Information Classification and Handling

4. SCOPE

Multi-disciplinary consultancy services including: Quantity surveying services, BIM, project management services, building surveyor services, geospatial surveying, principal designer and client advisor for CDM, Clerk of Works activities, building services design, sustainability consultancy, architectural design services, expert witness and advisory, property consultancy, structural engineering, geo-environmental services, civil engineering design, traffic and transportation planning, town and country planning. This is in accordance with the Statement of Applicability version 1.1 dated 02/02/2022.

5. ISMS OBJECTIVES

Ridge's ISMS objectives are designed to direct and support the achievement of an effective security programme, recognising security is a journey, and progress must be continually built upon. The objectives are set annually, and their progress monitored monthly.

The Objectives of the ISMS as of October 2021 are that:
- We achieve ISO 27001 certification.
- We operate the ISMS as originally designed.
- Our information risks are identified, managed, and treated in line with our risk management framework and risk appetite.
- Our Users and Administrators, accessing our information understand their information security responsibilities.
- Our ways of working consider information security.

6. ROLES AND RESPONSIBILITIES

Ridge will define, implement, and operate a governance risk and compliance structure suitable to information security management. This includes the identification and assignment of security roles and responsibilities to direct, control, operate, and monitor the ISMS. This includes:

- **An Information Security Board** - assigned with overall accountably for the ISMS performance.
- **An Information Security Partner Sponsor** - assigned with the duty of delegated authority for the for the ISMS performance.
- **The Risk Group** - to oversee the management of information security risks.
- **An Information Security Manager (Systems Manager)** - to manage the day-to-day operations of the ISMS.
- **IT specialists (RT Systems)** - to implement, operate and maintain the technical controls necessary of the ISMS.
- **Internal Audit Team** - to schedule and perform audits of the ISMS, determining its overall effectiveness.
- **Managers** - to ensure compliance to information security policy is maintained across their areas of responsibilities.

Everyone at Ridge has a personal responsibility for information security, this includes:

- Understanding and complying to this information security policy.
- Reporting suspected or actual security incidents to the IT Service Desk immediately upon discovery.
- Reporting security concerns to the IT Service Desk and seeking guidance from your Manager when you are unsure.
- Performing day-to-day activities with a security conscious mind-set.

7. COMPLIANCE MONITORING

Compliance with this policy and supporting policies and procedures will be monitored by Systems Team on an ongoing basis. Non-compliance to the policy will be reported through Ridge's Risk Management Framework and Disciplinary process.

The ISMS will comply will all legal and regulatory, and contractual requirements; underpinned by our commitment to the UK GDPR and achieving ISO 27001 certification.

Surveillance of the ISMS will be performed annually; by the Internal Audit department and external ISO 27001 Certification audit.

The ISMS documentation will be reviewed and updated, at yearly intervals, or where environment changes dictate.