Table of Contents

1. Purpose, scope and users

The aim of this Policy is to define the purpose, direction, principles and basic rules for information security management.

This Policy is applied to the entire Information Security Management System (ISMS).

Users of this document are employees of Ridgewall Ltd, as well as external parties who have a role in the ISMS.

2. Reference documents

- ISO/IEC 27001 standard, clauses 4.2.1 b) and A.15.1.1
- IS-P-001 IS Risk Assessment and Risk Treatment Procedure
- Statement of Applicability
- Master Services IT Document
- Legal Register
- POL-005 Business Continuity Management Policy
- IS-P-002 Information Security Incident Management Procedure
- Information Security Policies Handbook

3. Basic information security terminology*

Confidentiality - the property that information is not made available or disclosed to unauthorised individuals, entities, or processes

Integrity - the property of safeguarding the accuracy and completeness of assets

Availability - the property of being accessible and usable upon demand by an authorized entity

Information security (IS) - preservation of confidentiality, integrity and availability of information

Information Security Management System (ISMS) - that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

* Definitions taken from ISO/IEC 27001:2005

4. Information Security Management

4.1. Goals and objectives

Goals for the ISMS are to provide a structured approach to the protection of our information assets and minimise the potential for information security breaches to occur. To support these goals, information security objectives have been established and recorded in the IMS Objectives Programme. The goals and objectives are in line with the organisation's business objectives.

Downloaded or printed copies of this document are uncontrolled

The Technical Director is responsible for reviewing existing and setting new objectives. Individual security controls or groups of controls may be proposed by departmental heads, and approved by the Technical Director in the Statement of Applicability. The objectives must be reviewed at least once a year.

4.2. Information security requirements

This Policy and the ISMS shall meet relevant legal and regulatory requirements, as well as contractual obligations.

A detailed list of all contractual and legal requirements is provided in the Master IT Services Document and Legal Register.

4.3. Strategic risk management

Information risk management takes place as part of the business risk management and is in line with the organisation's strategic plans.

4.4. Risk evaluation criteria

Risk evaluation criteria are described in more detail in the Information Security Asset Inventory and Treatment Plan.

4.5. Business Continuity

Business continuity management is prescribed in the Business Continuity Management Plan – document reference ID-003

4.6. Responsibilities

Basic responsibilities for the ISMS are the following:

- the Technical Director has been appointed as the Information Security Officer with overall responsibility for the ISMS and for ensuring the ISMS is implemented according to this Policy
- the Technical Director is responsible for operational coordination and maintenance of the ISMS
- the Engineer in Charge is responsible for the technical implementation and support and for assisting with investigating reports of potential or actual security breaches
- the Directors must review the ISMS at least annually 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 Technical Director will implement information security training and awareness programs for employees
- the protection of integrity, availability, and confidentiality of individual information resource is the responsibility of the owner of the respective resource
- all security incidents or weaknesses must be reported in the first instance to the individuals line manager.

4.7. Policy communication

The Technical Director is responsible for ensuring that all employees of Ridgewall as well as external parties who have a role in the ISMS are familiar with this Policy. This Policy is made available to other interested parties on request.

Ridgewall communicates information security roles and responsibilities internally through the Responsibilities and Authorities section of The Hub and induction and direct communicatiron of any changes. Externally responsibilities and authorities are communicated through contracts and the RASCI table. Information Security Policies, principles and compliance requirements are explained in the Information Security Policies Handbook which is issued to all employees.

5. Support for ISMS implementation

The Directors of Ridgewall Ltd state that all phases in ISMS implementation will be supported with adequate resources in order to achieve the goals and objectives set in this Policy.

6. Validity and document management

The owner of this document is the Technical Director, who must review and if necessary update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- effective communication of this policy to employees and external parties who have a role in the ISMS
- compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organisation
- effectiveness of ISMS implementation and maintenance
- communication of responsibilities for ISMS implementation

7. Non-Compliance

Violation of any of the constraints of this Policy or its supporting policies and procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken including disciplinary action and possible suspension or restriction of rights and access to the IT systems.

This document is valid as of 13/07/2018

DIRECTORS:

Dominic McAnaspie
Alex Tillish
Mark Bonnamy
(signed copy available on request)