Top Level Information Security Policy

Revision	Author	Date	Approved By	Date
v1.0	Scott Gillham	June 2021		
V1.1	Scott Gillham	Aug 2021	Steve Sherry	Aug 2021

1. Introduction

This document is the top-level Information Security Policy adopted by Royal British Legion Industries (RBLI) and forms part of the organisation's Risk Management framework. The guiding principles and axioms described in this policy provide the basis for the more detailed information security policies, procedures and guidelines developed to manage specific security issues as they arise. These all form the Information Security Management System (ISMS). This document is the top-level policy that is written to align with ISO27001 with more detailed polices as annexes:

A.05 Information Security Policies

A.06 Organisation of Information Security

A.07 Human Resource Security

A.08 Asset Management

A.08 Access Control

A.10 Cryptography

A.12 Physical and Environmental Security

A.12 Operation Security

A.13 Communication Security

A.14 System Acquisition, Development and Maintenance

A.15 Supplier Relationships

A.16 Information Security Incident Management

A.17 Information Security aspects of business continuity management

A.18 Compliance

The Information Security Management System (ISMS) is more than a collection of documents. It is a systematic approach consisting of processes, technology and people that together work to protect and manage RBLI's information through effective risk management.

In order to protect its information, its stakeholder groups information from a range of internal and external threats. The term Stakeholder groups includes Beneficiaries, Residents and Tenants who could also be employees of RBLI.

This Information Security Management System Policy has been created to define the purpose, direction, principles and basic rules for this ISMS. It applies to the entire ISMS.

This policy applies to all employees of RBLI, as well as all external parties who have a role in the ISMS. Employees and external parties will be informed on their responsibilities in implementing this policy through procedures and training.

2. Definitions

The following defines some of the main terms referred to in this document.

Information Asset – RBLI's information and communications (ICT) systems and networks that store, process and communicate the electronic information that the organisation uses

and holds. This includes information itself in the form of computer data and print/non-print written materials.

Information Asset Owners – managers held accountable for the protection of particular Information Assets.

Information Security – the protection of information assets against threats to their confidentiality, integrity and/or availability.

ISO 27001 – ISO/IEC 27001 is an international standard on how to manage information security. The standard was originally published jointly by the International Organization for Standardization and the International Electrotechnical Commission in 2005 and then revised in 2013.

3. Policy summary

The confidentiality, integrity, security and availability of RBLI's information, and the information of its stakeholder groups, must always be preserved, whatever the form of the information and however it is shared, communicated, stored or otherwise processed, in a way that is compliant with applicable laws, regulations and contracts.

4. Guiding principles

RBLI's approach to information security is underpinned by the following seven fundamental principles.

1. The approach to information security management shall conform to accepted best practice as defined in the ISO 27000 series and other relevant information security standards.
2. Information is a critical business asset for RBLI and must be protected to a degree appropriate to its vulnerability and its importance to RBLI's activities, and to those of RBLI's external partners.
3. Information security controls are necessary to protect RBLI's information against unacceptable risks to their:
    - confidentiality (i.e. preventing the unauthorised disclosure of sensitive corporate or personal information),
    - integrity (i.e. ensuring that human errors, program deficiencies or faults do not reduce the completeness or accuracy of data) and
    - availability (i.e. minimising unplanned systems downtime that can result in the disruption of critical business processes).
4. RBLI's investment in proven information security controls are justified on the basis of lifecycle cost-benefit assessment and risk analysis. The aim is not the complete elimination of information security risks but to minimise them in the most cost-effective manner, offsetting the cost of controls against the anticipated reduction in losses due to the avoidance or mitigation of security incidents.
5. Information security is pervasive throughout the whole organisation and is an inherent part of RBLI's IT infrastructure, operational and management processes. It is considered more than an "IT matter" and the information security management system (ISMS) shall be regarded and managed as an integral part of the organisation's management framework.

6. Information management is a core element of corporate governance. It is aligned to IT management, physical site security, risk management, legal and regulatory compliance and business continuity.

7. Information security is a business enabler that allows the organisation to enter more confidently into and maintain business relationships, markets and situations that would otherwise be too risky, or which might not have presented an opportunity if information security is sub-standard. By minimising financial losses resulting from information security incidents, it supports the bottom line whilst enhancing RBLI's image as a trustworthy, open, honest and ethical organisation.

5. Scope

The scope of the RBLI Security Policies is applicable to the following and is in accordance with the Statement of Applicability (available in the ISMS):

a. Processes and services

- Manufacturing
- Housing
- Care
- Internal business

b. Organisation units

- Britain's Bravest Manufacturing Company
- Scotland's Bravest Manufacturing Company
- RBLI Living
- Strategic Development
- Corporate Service

c. Assets

- RBLI information
- Stakeholder information
- Processes and Intellectual Properties
- People
- Reputation and brand
- Equipment
- Facilities
- Management of outsourced services

d. Locations

The ISMS applies to all parts of the organisation that is used by RBLI staff to access, store or process data, these locations are:

HEAD OFFICE:

- **Royal British Legion Industries,**

  Hall Road, Aylesford, Kent, ME20 7NL

SOCIAL ENTERPRISES BBMC AND SBMC

- **BBMC Kent**

Royal British Legion Industries, Hall Road, Aylesford, Kent ME20 7NL

- **BBMC Surrey**

  Bradmere House, Brook Way, Kingston Road, Leatherhead, KT22 7N

- **SBMC Scotland**

  Bishopton, Renfrewshire, Scotland, PA7 5PU

RBLI VILLAGE

- **Gavin Astor House**

  Royal British Legion Village, Aylesford, Kent, ME20 7NF

- **Queen Elizabeth Court**

  Admiral Moore Drive, Aylesford, Kent, ME20 7SU

- **Mountbatten Pavilion**

  Admiral Moore Drive, Aylesford, Kent, ME20 7SE

- **Base Camp**

  Hall Road, Aylesford, Kent, ME20 7NL

- **Appleton Lodge Care Home**

  14 Milner Road, Royal British Legion Industries Village, Kent, ME20 7FU

- **Capel Morris Centre – Community, Events and Sports Centre**

  Hall Road, Aylesford, Kent, ME20 7NL

REMOTE WORKING

In addition to the listed properties above RBLI also has external locations such as employment offices and staff working from home. These locations are included in the ISMS and come under the remote working policies.

e. Exclusions from scope

RBLI owns properties that are rented to tenants and are personal dwellings. All residential properties that are rented as a home and are not allocated as a workplace are excluded from scope. For clarification a care home has residents and allocated staff, so it included in the scope. A rented home to a person or family is not included.

The processes around the maintenance and tenancy of properties are included in the ISMS, but the properties themselves are considered external to RBLI for the sake of information security. This includes Prince Philip Lodge and the rented housing.

6. Information Security Management

a. Objectives and measures

The high level objectives for the RBLI ISMS are as follows, a more detailed document exists in the ISMS that includes the measuring of the factors that will determine if these objectives are being achieved:

ID	Objective	Measure

1	Ensure RBLI is not subject to a damaging security breach	Information security reporting records: RBLI is not subjected to any incident that requires reporting to a regulatory authority. AND RBLI is not subjected to an incident that impacts RBLI's ability to fulfil its contracts and obligations
2	Ensure all staff are trained appropriately in their role to fulfil their part of the ISMS to protect RBLI's information	Training records, Information security reporting records, personal development process Infosec@rbli.co.uk for support regarding information security in RBLI.
3	Provide RBLI the ability to win contracts that require security accreditation	RBLI accredited to ISO27001 and maintained its accreditation going forward
4	Provide confidence to all RBLI stakeholders and external parties that information security is appropriately managed and controlled	dpo@rbli.co.uk email for data protection communications and data subject rights.

b. Information security requirements

This policy and the entire ISMS must be in line with the legal and regulatory requirements relevant to RBLI, as well as with contractual obligations.

c. Strategic risk management

Information risk management takes place as part of business risk management in line with RBLI's strategic direction.

d. Risk evaluation criteria

Risk evaluation criteria are described in more detail in the Risk Management Process (Assessment and Treatment) reference document.

e. Business continuity

Business continuity management is prescribed in the Business Continuity Management Policy.

f. Responsibilities

The Board of Trustees are ultimately accountable for corporate governance as a whole and responsible for ensuring the ISMS is adequately funded and resourced. The management and control of information security risks is an integral part of corporate governance. In practice, the Board of Trustees explicitly delegate executive responsibilities for most governance matters to the Senior Management Team, led by the Chief Executive.

This top-level policy applies throughout the organisation as part of RBLI's risk management framework. It applies to all RBLI employees, contractors or other third parties acting in a similar capacity, whether they are explicitly bound by contractual terms and conditions or implicitly bound by, for example, generally accepted standards of acceptable behaviour.

The RBLI Security organisation documents the team responsible for implementing the ISMS. The responsibilities of this teams include:

- Implement and maintain this Information Security Management System Policy, as well as the procedures, policies and other documentation required to support it.
- The operational co-ordination of the ISMS and its continuous improvement Review the ISMS at least once a year, or in the event of significant change, and prepare minutes from that meeting. The purpose of this review is to establish the suitability, adequacy and effectiveness of the ISMS, including the objectives.
- Information security training and awareness programs
- The confidentiality, integrity, security and availability of individual assets
- Objectives and measures are identified and implemented
- Any information security breach or weakness must be reported immediately

All employees will be responsible and accountable for information security relevant to their roles. Violations of this or any related policy or procedure by any employee may result in disciplinary action and/or dismissal and/or criminal prosecution. Breaches of information security will not be tolerated

g. Policy communication

RBLI will ensure that all employees of RBLI, as well as external parties who have a role in the ISMS, are familiar with this policy.

7. Support for ISMS Implementation

The SMT are committed to ensuring that all phases in ISMS implementation will be supported with adequate resources in order to achieve all objectives set out in this policy.

8. Reference documents

- ISO/IEC 27001, cl 4.2.1(b) and A15.1.1
- Statement of applicability
- RBLI Security Organisation
- Risk management process (Assessment and Treatment)
- List of statutory, regulatory and contractual obligations
- Business Continuity Management Policy
- Incident Management Procedure

9. Validity and document management

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

- Number of employees and external parties who have a role in ISMS, but are not familiar with this document
- Non-compliance with laws, regulations and contractual obligations
- Ineffectiveness of ISMS implementation and maintenance
- Unclear responsibilities for ISMS implementation

10. Continual Improvements

As with other management systems standards, an essential part of an Information Security Management System is that of continual improvements. The identification and treatment of information security risks and the associated processes shall be used to identify and implement improvements using the Plan→Do→Check→Act (the "PDCA Cycle") model of continual improvement. Opportunities for improvement shall be assessed before being implemented and the outcomes recorded and reported to ensure the effectiveness of the ISMS.

11. Supporting Documentation

This Policy shall be supported by additional documentation in the ISMS in accordance with ISO27001:2013

12. Applicability

This top-level policy shall be reviewed and evaluated annually and also when changes occur within the business, or through external circumstances that may affect a particular approved policy statement.