A06 Organisation of Information Security

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

Purpose

This policy is intended to ensure that a management framework is in place to initiate, plan and control the implementation and operation of information security within the organisation.

6.1 Internal organisation

All key persons responsible for the security of each client assignment/service must be documented, including those within customer/supplier/third party organisations (see RBLI Roles and Responsibilities document and BSAU).

6.1.1 Management information security roles & responsibilities

Security is the responsibility of everyone. All persons involved must be able to express their opinion in an appropriate forum, details of this will be included in staff training. The RBLI Security Organisation Document identifies the key staff and roles and will be maintained for all staff/role changes. The following table summarises the key roles and responsibilities in RBLI's information security management.

Person	Roles & Responsibilities
Board of Trustees	The RBLI Board of Trustees is ultimately accountable for the management and control of information security risks as an integral part of corporate governance.
Chief Executive	Overall responsibility for ensuring that RBLI complies with all relevant information security legislation and follows best practice. Approves all strategy documents and Policy Statements and, as necessary, other relevant documents.
Senior Management Committee	The RBLI SMT give overall strategic direction by approving and mandating the information security principles
Head of Corporate Governance	Overseeing the development of and compliance with the policy framework. Engaging with Senior Management to aid review and maintenance of key documentation.
Data Protection Team	Operational responsibilities for information security is delegated to the data protection team (Head of Corporate Governance, Head of Business Systems and ISO27001 Project Manager) who will work with the rest of the RBLI organisation to establish the information security management system to implement ISO27001
All staff	Working within the current policies, procedures, and guidelines in use and specific to their area of work.

6.1.2 Segregation of Duties.

Any need to separate duties must be documented in the information security risk assessment and documented in the appropriate policy/procedure. This may be required to reduce opportunities for

unauthorised or unintentional modification or misuse of RBLI assets. Segregation of duties is identified in the risk assessment which will inform where segregation is necessary and be reflected into procedures as appropriate.

6.1.3 Contact with Authorities

RBLI must maintain appropriate levels of contact with regulatory bodies, information service providers to ensure that appropriate action can be taken quickly in the event of a security incident. See the Information Security Data Breach Incident Response Procedure for further details.

6.1.4 Contact with Special Interest Groups

Where required RBLI will maintain contact with specialist security forums, groups or professional associations. In the Applicable Legislation and Contractual requirements Register,, part of this ISMS, other RBLI obligations are documented

6.1.5 Information Security in project management

Information security shall be addressed in project management, regardless of the type of the project. A risk assessment on every project will be conducted to determine its potential impact on information security.

All planned changes to the RBLI Information infrastructure must be agreed with the Head of Business Systems who is responsible for determining if an Information Security Policy risk assessment is required.

Access to RBLI's infrastructure and information systems is restricted to its staff and any approved external person or agency (who must agree to the RBLI security policy before being provided access).

The RBLI BSAU will hold a record of all persons and organisations approved for secure access to information and systems.

6.2 Mobile devices and Teleworking

6.2.1 Mobile computing and Teleworking

Mobile working systems are particularly vulnerable and specific security controls must be identified in the Information security risk assessment.

RBLI will follow industry best practice is to make use of VPN or similar encryption software to protect the transactions and good physical security, on the computers and communications systems used to contact the corporate information space. Good personal security policies – use of passwords, use of encrypted file systems as available with operating systems will also be implemented.