Records Retention and Protection Policy

Revision	Author	Date	Approved By	Date
v1.0	Mike Smith	May 2018	Philip Defraine	May 2018
V1.1	Kate Porter	Jul 2021	Lisa Farmer	Aug 2021

1. Introduction

In its everyday business operations, RBLI collects and stores records of many types and in a variety of different formats. The relative importance and sensitivity of these records also varies and is subject to the organisation's security classification scheme.

It is important that these records are protected from loss, destruction, falsification, unauthorised access and unauthorised release, and a range of controls are used to ensure this, including backups, access control and encryption.

RBLI also has a responsibility to ensure that it complies with all relevant legal, regulatory and contractual requirements in the collection, storage, retrieval and destruction of records. Of particular relevance is the European Union General Data Protection Regulation (GDPR) and its requirements concerning the storage and processing of personal data.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers, contractors and other third parties who have access to systems.

2 Records Retention and Protection Policy

This policy begins by establishing the main principles that must be adopted when considering record retention and protection. It then sets out the types of records held by and their general requirements before discussing record protection, destruction and management.

2.1 General Principles

There are a number of key general principles that must be adopted when considering record retention and protection policy. These are:

- Records must be held in compliance with all applicable legal, regulatory and contractual requirements
- Records must not be held for any longer than required
- The protection of records in terms of their confidentiality, integrity and availability must be in accordance with their security classification
- Records must remain retrievable in line with business requirements at all times
- Where appropriate, records containing personal data must be subject as soon as possible to techniques that prevent the identification of a living individual, for example anonymization, aggregation.

2.2 Record Types and Guidelines

In order to assist with the definition of guidelines for record retention and protection, records held by RBLI are grouped into the categories listed in the table on the following page. For each of these categories, the required or recommended retention period and allowable storage media are also given, together with a reason for the recommendation or requirement.

Note that these are guidelines only and there may be specific circumstances where records need to be kept for a longer or shorter period of time. This should be decided on a case by case

basis as part of the design of the information security elements of new or significantly changed processes and services.

2.3 Use of Cryptography

Where appropriate to the classification of information and the storage medium, cryptographic techniques must be used to ensure the confidentiality and integrity of records.

Care must be taken to ensure that encryption keys used to encrypt records are securely stored for the life of the relevant records and comply with the organisation's policy on cryptography.

2.4 Media Selection

The choice of long term storage media must take into account the physical characteristics of the medium and the length of time it will be in use.

Where records are legally (or practically) required to be stored on paper, adequate precautions must be taken to ensure that environmental conditions remain suitable for the type of paper used. Where possible, backup copies of such records should be taken by methods such as scanning. Regular checks must be made to assess the rate of deterioration of the paper and action taken to preserve the records if required.

For records stored on electronic media such as tape, similar precautions must be taken to ensure the longevity of the materials, including correct storage and copying onto more robust media if necessary. The ability to read the contents of the particular tape (or other similar media) format must be maintained by the keeping of a device capable of processing it. If this is impractical an external third party may be employed to convert the media onto an alternative format.

2.5 Record Retrieval

There is little point in retaining records if they are not able to be accessed in line with business or legal requirements. The choice and maintenance of record storage facilities must ensure that records can be retrieved in a usable format within an acceptable period of time. An appropriate balance should be struck between the cost of storage and the speed of retrieval so that the most likely circumstances are adequately catered for.

2.6 Record Destruction

Once records have reached the end of their life according to the defined policy, they must be securely destroyed in a manner that ensures that they can no longer be used. The destruction procedure must allow for the correct recording of the details of disposal which should be retained as evidence.

2.7 Record Storage & Retention

The following summarises the main categories of records, reasons for retentions and the allowable storage media. This should be reviewed to establish whether these are still applicable in terms of legal, operational and organisational requirements.

Retention Category	Description	Retention Period	Mandatory Y/N	Note	Allowable storage media
Accounting	Invoices, purchase orders, accounts and other historical financial records	6 years after expiry	Y		Electronic/paper
Budgeting and forecasting	Forward looking financial estimates and plans	6 years after expiry	N		Electronic/paper
System transaction logs	Database journals and other logs used for data recovery	3 months	N	Sota facility maintain logs, operational procedures etc	Electronic
Audit logs	Security logs – e.g. records of logons and logoffs	3 months	N		Electronic
Operational procedures	Records associated with the completion of operational procedures	3 months	N		Electronic/paper
Customer	Personal data, including customer names. Addresses, order history, credit card and bank details	6 years after last purchase	Y	Data protection requirement	Electronic/paper
Supplier	Supplier names, addresses, company details	6 years after ;last supply	Y	Maximum period within which each dispute might occur	Electronic/paper
Human resources	Employee names, addresses, bank details, tax codes, employment history	6 years but 12 years recommended	Y	Data protection requirement and employment law	Electronic/paper
Contractual	Legal contracts, terms and conditions, leases	12 years	Y	Maximum period within which dispute might occur	Electronic/paper
Care	Resident names, health conditions, care requirements	8 years	Y	Data protection requirement	Electronic paper
Mailing Lists	Email Address	2 years after last contact	Y	Data protection requiment	Electronic
Supporters	Name, address, email address, financial information	6 year	Y	Data Protection requirement	Electronic/Paper

2.8 Record Protection and Management

All data on RBLI servers will be held securely on encrypted servers in a data centre. These servers will be securely backed up and replicated to ensure data is protected.
Access to records will be controlled by Active Directory permissions and permissions are only granted when requested or authorised by management of the business area.