1. **Scope** [ISO27002 Clause 18.1.3]

All Retirement Capital’s records, whether analogue or digital, are subject to the retention requirements of this procedure.

1. **Responsibilities**

The Managing Director is responsible for retention of financial (accounting, tax) and related records.

The Company Administrator is responsible for retention of all HR records.

The Director (CISO) is responsible for retention of all Health and Safety records, etc.

The Managing Director is responsible for retention of all other statutory and regulatory records.

The Company Administrator is responsible for storage of data in line with this procedure.

Each Department Manager is responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

1. **Procedure**

* 1. The required retention period for the company is seven years for all record types, see: [ISMS-DP-DOC 19.4](file:///I:\Shared%20drives\Company\Quality\QMS\ISMS\06%20Data%20Protection\ISMS-DP-DOC-19.4.docx), Data Retention Policy
  2. Each data item that is stored is marked electronically or by means of a sticky label with the name of the record, the record type, the original owner of the data, the information classification, the data of storage, the required retention period, the planned date of destruction, and any special information (e.g. in relation to cryptographic keys).
  3. Cryptographic keys, which are required for sensitive data are retained as set out in [ISMS-C DOC 10.1.2](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A10\ISMS-C_DOC_10.1.2.docm).
  4. For all electronic storage media, Retirement Capital retains the means to access that data, see: [ISMS-DP-DOC 19.4](../Section%2011%20-%20data%20protection/ISMS-DP-DOC-19.4.docx), Data Retention Policy
  5. For all electronic storage media, Retirement Capital does not exceed 90% of the manufacturer’s recommended life. The Change Manager has a schedule that identifies, for each of the storage media in use, what this recommended life is and which cross-references to the table above. When the 90% of expected life mark is reached, the Change Manager duplicates the stored data onto new storage media.
  6. The Change Manager is responsible for destroying data once it has reached the end of the retention period specified in 3.1 above. Destruction must be completed within 30 days of the planned retention period. Destruction is handled as laid out in Work Instruction [ISMS-C-DOC 11.2.7](file:///I:\Shared%20drives\Company\Quality\QMS\ISMS\03Z%20Validated%20DOCX%20files\Control%20A11%20-%20physical%20and%20environmental%20security\ISMS-C_DOC_11.2.7.docx)

***Document Owner and Approval***

The Managing Director is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This procedure was approved by the Chief Information Security Officer on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature:

Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |