# Compliance and Retention of Records

Reference: DSP DOC 01-1.7.4
DocumentKits Issue No: 1.1
Organisation Issue No:
DocumentKits Issue Date: 23/02/2021
Organisation Issue Date:

**1. Scope**

Organisation Name's information assets and any information assets owned by a third-party that Organisation Name supports.

All Organisation Name's records are subject to the retention requirements of this procedure.

**2. Responsibilities**

2.1 All Employees/Staff of Organisation Name have specific compliance responsibilities.

2.2 The Chief Information Security Officer (CISO) is responsible for software and system audits.

2.3 The Board of Directors is responsible for retention of records.

**3. Procedure**

3.1 Legal, statutory and other requirements – general:

3.1.1 The Board of Directors retains a list of applicable statutory and regulatory requirements relevant to Organisation Name's information systems. The Board of Directors reviews this list annually, updating it as appropriate, and ensures that any activities undertaken do not contravene any of the regulations and statutes prevailing. Appropriate staff training and awareness is provided as necessary.

3.1.2 Organisation Name will protect its own and other parties' intellectual property through control over access to information and the proper licensing of information and software.

<<3.1.3-3.1.4 removed for sample purposes>>

3.2 Copyright

SAMPLE

3.2.1 Copying (including duplicating and any other variant of the copying concept) of anything (whether document, digital asset, software, or anything else) other than in line with UK copyright law is explicitly forbidden.

3.2.2 Software and other third-party copyrighted items may only be obtained through legitimate suppliers, and only on the basis that the software or copyright licence terms will be complied with, including as to numbers of users/basis of sale, etc. Organisation Name will maintain a software and copyright asset register together with copies of software licences, etc. From time to time, internal audits will be carried out to ensure no unlicensed software has been installed and that the maximum number of user licences has not been exceeded.

3.2.3 Organisation Name's copyright ownership of documents (including drawings, charts, etc., owned or originated by Organisation Name, or contributed to or originated by third parties under contract to Organisation Name, including contractors, teleworkers and Employees/Staff during their employment) should be established through contracts.

<<3.2.4-3.2.6 removed for sample purposes>>

3.3 Trademarks

3.3.1 Top Management will identify where it is appropriate for Organisation Name to register trademarks.

3.3.2 All trademarks, whether or not registered, are listed and will be managed by the Board of Directors.

3.3.3 The Board of Directors will take appropriate action, including legal action where necessary, to protect its trademarks from infringement.

3.4 Data protection and privacy

See the Data Protection and Confidentiality Policy.

3.5 Record retention

3.5.1 The required retention periods, by record type, are below:

**Record type:** HR record
**Retention period:** 6 years
**Responsible:** Chief Executive Officer (CEO)

SAMPLE

**Record type:** Finance data
**Retention period:** 6 years
**Responsible:** Chief Executive Officer (CEO)

**Record type:** Customer data
**Retention period:** 6 years
**Responsible:** Head of IT (CIO)

**Record type:** Incident documents
**Retention period:** 3 years
**Responsible:** Chief Information Security Officer (CISO)

**Record type:** Property lease documents
**Retention period:** 2 years
**Responsible:** Chief Executive Officer (CEO)

<<Content removed for sample purposes>>

**Record type:** Health and care records
**Retention period:** The specific retention requirements for health and care records are listed in the Records Management Code of Practice for Health and Social Care 2016 in its detailed retention schedule. (This document is updated regularly.)

3.5.2 The Manager/Executive (genericline) is responsible for destroying data once it has reached the end of the retention period. Destruction must be completed within 90 days of the planned retention period.

3.5.3 Organisation Name uses audit tools for system audits, and the Head of IT (CIO) is responsible for protection of information system audit tools.

***Document owner and approval***

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the Master List of Document Approval.

SAMPLE