

[Company]

DATA RETENTION POLICY

Retention of Information

1 Document Version Control

Last Modified		Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

1	Document Version Control.....	2
2	Document Contents Page.....	3
3	Data Retention Policy	5
3.1	Purpose	5
3.2	Scope.....	5
3.3	Principle	5
3.4	Agreement of Retention Periods.....	6
3.5	Record of Retention Periods.....	6
3.6	Expiry of Retention Period	6
3.7	Suspension of Record Disposal in the event of litigation or claims	7
4	Policy Compliance	8
4.1	Compliance Measurement	8
4.2	Exceptions	8
4.3	Non-Compliance	8

4.4 Continual Improvement.....8

3 Data Retention Policy

3.1 Purpose

The purpose of this policy is to ensure that necessary records, documents, and information of the company containing personal data are retained for no longer than necessary for the purposes for which personal data are processed.

3.2 Scope

All employees and third-party users.

Personal Data as defined by GDPR.

3.3 Principle

The GDPR principle of Data Storage Limitation for personal data.

3.4 Agreement of Retention Periods

The relevant owners of the documentation as detailed in the asset register are responsible for agreeing the data retention periods in line with legal, regulatory, and business requirements.

Data retention periods are approved by legal counsel.

3.5 Record of Retention Periods

Retention periods are recorded in the Data Asset Register. Additional detail is contained where applicable and appropriate in the Record of Processing Activities and the Asset Register.

3.6 Expiry of Retention Period

When the retention target is reached, the information will be reviewed by relevant owners of the documentation as detailed in the asset register to confirm that the information is to be further retained or destroyed. It will be destroyed in line with the Information Classification and Handling Policy if there is no further business, statutory or historical reason to keep them or to select them for re review at a later date; either because the business need is ongoing or because of potential historical value.

3.7 Suspension of Record Disposal in the event of litigation or claims

In the event any employee of the company reasonably anticipates or becomes aware of a governmental investigation or audit concerning the company or the commencement of any litigation against or concerning the company, such employee shall inform Directors and Board of Directors and any further disposal of documents shall be suspended until such time as the Board of Directors, with the advice of the Executive Director and the company legal counsel, determines otherwise. The Directors shall take such steps as are necessary to promptly inform affected staff of any suspension in the disposal or destruction of documents.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.