Document Retention Policy

Governance Policy | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to “the Company” with your organisation’s name.

Document Control

Document name	Document Retention Policy
Document type	Governance Policy
Jurisdiction	Global
Owner	Company Secretary
Approved by	Board of Directors
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose

This Policy establishes the Company's requirements for the creation, classification, retention, storage, retrieval and destruction of records. Records are corporate assets: they evidence the Company's decisions and transactions, enable it to meet legal and regulatory record-keeping obligations in each jurisdiction in which it operates, support the defence and prosecution of legal claims, and allow regulators, auditors and customers to be answered accurately and promptly.

The Policy has two complementary objectives. First, records must be retained for at least the minimum periods required by applicable law and kept accessible, complete and unaltered for the whole of those periods, consistent with ISO 15489 and, for customer and transaction records, FATF Recommendation 11. Second, records — particularly those containing personal data — must not be retained indefinitely: once no retention obligation or legitimate business need remains, records must be securely destroyed or de-identified, consistent with the storage limitation principle reflected in the OECD Privacy Guidelines and the GDPR. Over-retention increases privacy, cyber and discovery risk and is itself a compliance failure under most modern data protection regimes.

This Policy has been approved by the Board of Directors. It is owned and administered by the Company Secretary and is reviewed annually. It should be read together with the Company's Privacy Policy, Information Technology Security Policy, Data Governance Policy and Business Continuity Management Policy.

2. Scope

This Policy applies to the Company and all of its subsidiaries and controlled entities, and to all directors, officers, employees, secondees, contractors, consultants and agents (together, "staff"). It applies across all business lines, products, channels and functions.

The Policy covers records in every format and location, including:

- paper documents, files, books, plans and registers;
- email, calendar entries, instant messages, chat and collaboration-platform content (including approved messaging channels used for business purposes);
- data held in core banking, lending, payments, CRM, HR, finance and risk systems, including database entries and system logs;
- voice recordings, images, video and scanned documents; and
- records held on the Company's behalf by service providers, including cloud storage and software-as-a-service platforms.

Transitory records are within scope only to the extent that they must not be disposed of while subject to a Legal Hold. Personal records of staff that do not relate to the Company's business are out of scope; however, staff must not use personal accounts, devices or applications to create or store Company records

(see the Prohibited storage requirements in the Storage, Format and Integrity section).

2.1 Jurisdictional application

This Policy states international best practice drawn from ISO 15489, the FATF Recommendations, the Basel Framework and internationally recognised privacy principles. The Company must map the requirements of this Policy — in particular the minimum retention periods, destruction rules and privacy obligations — to the law of each jurisdiction in which it operates, and must record the applicable local periods in the Retention Schedule and the System-of-Record Register. Where the law of an operating jurisdiction imposes a stricter or additional requirement, local law prevails over this Policy.

3. Definitions

Term	Definition
Record	Any information created, received or maintained by the Company as evidence of, or in the course of, its business activities, in any format — including paper documents, emails, instant messages and chat transcripts, system and database entries, voice recordings, images, spreadsheets, collaboration-platform content and structured data feeds.
Record Class	A grouping of records with common regulatory, business and evidentiary characteristics that attracts a common minimum retention period under the Retention Schedule.
Retention Period	The minimum period for which a record class must be preserved, measured from the trigger event specified in the Retention Schedule (for example, transaction completion, end of customer relationship or end of employment).
Retention Schedule	The table in the Retention Schedule section of this Policy setting the minimum retention period, trigger event and legal or regulatory basis for each record class, as localised to each jurisdiction in which the Company operates.
System of Record	The single application, repository or physical archive designated in the System-of-Record Register as the authoritative source for a record class; copies held elsewhere are convenience copies only.
System-of-Record Register	The register maintained by the Company Secretary listing each record class, its

	system of record, its Information Asset Owner, its retention period and its destruction method.
Information Asset Owner	The executive or senior manager accountable for a defined information asset, group of information assets or record class, including its classification, accuracy, access decisions, risk acceptance, storage, retention, retrieval and eventual destruction.
Legal Hold	A written direction, ordinarily issued by the General Counsel, suspending the routine destruction, deletion, alteration or overwriting of specified records, communications and data that are, or may reasonably become, relevant to litigation, a dispute, an investigation, an audit or a regulatory or supervisory request.
Destruction	The permanent and irreversible disposal of a record such that it cannot be read, reconstructed or recovered by any reasonably available means.
De-identification	The permanent removal or alteration of personal data within a record so that no individual is identifiable or reasonably identifiable from the remaining information, having regard to all means reasonably likely to be used to re-identify it.
Personal Data	Any information relating to an identified or identifiable natural person, whether accurate or not and in whatever form recorded, including identifiers such as name, account and identification numbers, location data, online identifiers and factors specific to that person's identity, consistent with the OECD Privacy Guidelines and applicable data protection law. The terms personal data and personal information are used interchangeably.
Metadata	Data describing a record's context, content and structure — including author, creation date, modification history, transmission details and system audit trails — which may itself be required to establish a record's authenticity, reliability and admissibility.
Migration	The controlled transfer of records from one format, medium or system to another in a manner that preserves content, context, metadata and evidentiary

	integrity.
Transitory Record	Material of no ongoing business, legal or evidentiary value — such as duplicates, personal notes not used in decision-making, and superseded drafts containing no substantive information absent from the final record — which may be disposed of without formal destruction approval unless subject to a Legal Hold.
Certificate of Destruction	A written attestation, issued by the person or service provider carrying out destruction, identifying the records destroyed, the method used, the date and the authorising approval.
Limitation Period	The period prescribed by applicable law within which a civil claim must be commenced, after which it is generally barred; a key input when setting retention periods beyond regulatory minimums.

4. Regulatory Framework

The key legislation, regulations and standards relevant to this document include (as amended from time to time):

Instrument / Standard	Relevance
ISO 15489-1:2016 Information and documentation — Records management	The international benchmark for records management: records must be authentic, reliable, complete and usable, with systematic controls over creation, capture, classification, retention and disposition — the framework this Policy implements.
FATF Recommendations, Recommendation 11 (Record-keeping)	Requires financial institutions to keep all necessary transaction records and customer due diligence material for at least five years after the transaction or the end of the business relationship, sufficient to permit reconstruction of individual transactions and to respond swiftly to competent-authority requests.
FATF Recommendation 10 (Customer due diligence)	Underpins the customer identification and verification records that must be captured and retained under the AML/CFT record class in the Retention Schedule.
BCBS Principles for the Sound Management of Operational Risk (revised 2021)	Requires banks to maintain documentation of processes, controls, incidents and decisions sufficient to manage operational risk — records management failures are themselves an

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.

finance-policies.com