

Data Retention Policy

Policy Statement

World Bank shall define, implement, and rigorously enforce data retention schedules for all categories of its business records and information, encompassing both electronic data and physical documents. This policy is established to ensure compliance with all applicable legal, regulatory, operational, and business requirements, while concurrently minimizing data-related risks, optimizing storage resources, and ensuring the timely and secure disposal of data that is no longer required.

Scope

This policy applies universally to all data created, received, processed, or stored by World Bank systems, by its employees, and by third-party entities acting on its behalf. This scope covers data across all media types, including structured data in databases, unstructured data in documents and emails, data on servers, workstations, mobile devices, removable media, and data residing in cloud services.

Roles and Responsibilities

The effective implementation of this Data Retention Policy relies on clearly defined roles and responsibilities:

- **Data Owners:** Typically senior managers or department heads, Data Owners are responsible for defining appropriate retention periods for the data assets within their specific business or functional domain. This determination is made in close consultation with the Legal, Compliance, and IT departments to ensure all requirements are met. They are also responsible for authorizing data disposal at the end of its lifecycle.
- **Legal Department:** Provides authoritative guidance on all legal and regulatory retention requirements applicable to World Bank's global operations. This includes interpreting laws such as SEC Rule 17a-4 , FINRA rules , GDPR , and other relevant national and international statutes. The Legal Department also manages legal hold processes.
- **Compliance Department:** Ensures that the Data Retention Policy and its implementation align with all applicable regulatory mandates and internal compliance standards. They conduct periodic reviews and audits of retention practices.
- **IT Department (Data Custodians):** Responsible for the technical implementation and management of data retention, archiving, and secure disposal mechanisms across World Bank's IT systems. This includes configuring systems to enforce retention rules, managing archive storage, and executing secure data deletion procedures.

- **Security Manager / Cybersecurity Team:** Ensures that appropriate security controls are applied to all retained and archived data, protecting it from unauthorized access, modification, or disclosure throughout its lifecycle. They also advise on secure disposal methods.
- **All Employees:** Responsible for understanding and adhering to this policy in their daily handling of World Bank data, including proper record creation, storage, and identification for disposal when appropriate.

Key Principles

World Bank's Data Retention Policy is founded on the following core data governance principles, largely derived from regulations like GDPR Article 5 :

- **Lawfulness, Fairness, and Transparency:** Data is retained only for legitimate and lawful purposes, and processes related to retention are transparent to relevant stakeholders, including data subjects where applicable.
- **Purpose Limitation:** Data is collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. Retention periods are tied to these original purposes.
- **Data Minimization:** Only data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed and retained will be kept. Redundant, obsolete, or trivial (ROT) data is actively managed and disposed of.
- **Accuracy:** Reasonable steps are taken to ensure that retained data is accurate and, where necessary, kept up to date. Inaccurate data is rectified or erased.
- **Storage Limitation:** Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed. Once the defined retention period expires, data must be securely disposed of or anonymized.
- **Integrity and Confidentiality (Security):** Retained data is protected by appropriate technical and organizational security measures against unauthorized or unlawful processing, accidental loss, destruction, or damage.
- **Accountability:** World Bank will be able to demonstrate compliance with these principles.

Procedures

- **Data Classification:** All World Bank data must be classified according to its sensitivity, criticality, and regulatory implications (as defined in the Bank's Data Classification Policy). This classification is a primary input for determining appropriate retention

periods and handling requirements. Financial records and customer PII, for instance, will typically have more stringent retention and security requirements.

- **Retention Schedule Development and Maintenance:**

- A comprehensive, Bank-wide Data Retention Schedule must be developed, maintained, and regularly reviewed (at least annually) by Data Owners in collaboration with Legal, Compliance, and IT.
- This schedule must specify the minimum and, where applicable, maximum retention periods for each distinct category of data (record type).
- *Example Data Categories for World Bank:* Customer identification program (CIP) records, transaction records, loan origination and servicing documents, international trade finance documentation, financial statements, internal and external audit reports, email and other electronic communications, employee records, system and security logs, vendor contracts, research data, and project documentation.
- *Example Retention Periods (Illustrative, to be confirmed by World Bank Legal/Compliance based on specific jurisdictions and activities):*
 - Customer Account Records (e.g., applications, agreements, statements): Typically 5-7 years after account closure, subject to local regulations (e.g., SEC Rule 17a-4 suggests 6 years for broker-dealers).
 - Transaction Records (e.g., wire transfers, loan payments): Often 5-10 years, depending on AML/CFT regulations and specific transaction types.
 - General Business Correspondence (Email): 3-7 years, depending on content and relevance to specific transactions or legal matters (FINRA rules suggest 3 years for general communications for broker-dealers).
 - Financial Statements (Audited Annual Reports): Permanent.
 - Internal Audit Reports: Typically 7-10 years, or as per internal governance requirements.
 - Security Event Logs: Minimum 1 year, with critical security incident logs retained longer for forensic purposes (PCI DSS, for example, requires 1 year with 3 months immediately available).

- **Data Archiving:**

- Formal procedures must be established for archiving data that is no longer in active operational use but must be retained to meet legal, regulatory, or long-term business requirements.

- Archived data must be stored in a secure, controlled, and cost-effective environment.
- Archived data must remain indexed and accessible for timely retrieval in response to legal discovery requests, regulatory inquiries, or internal audits. The accessibility requirements of SEC Rule 17a-4 ("easily accessible place" for the first two years) should be considered for relevant records.

- **Secure Disposal:**

- Formal procedures must be implemented for the secure and irreversible deletion or destruction of data once its mandated retention period has expired and it is not subject to any active legal hold.
- Disposal methods must be appropriate to the sensitivity of the data and the nature of the storage media, adhering to standards such as NIST SP 800-88 (Guidelines for Media Sanitization – Clear, Purge, Destroy). For sensitive financial data, "Purge" or "Destroy" methods are typically required.
- Records of data disposal (Certificates of Destruction) must be maintained as an audit trail.
- *Security Manager's Perspective:* At World Bank, automated data deletion workflows are implemented for certain structured data types (e.g., expired web server logs) once their retention period is met. However, these automated processes are subject to stringent pre-deletion verification protocols, exception handling for data under legal hold, and comprehensive audit logging to prevent the accidental or unauthorized loss of critical institutional records. For unstructured data and physical records, disposal is a more manually verified process managed by designated custodians.

- **Legal Holds (Litigation Holds):**

- A distinct process must be in place to identify, preserve, and prevent the destruction or modification of data that is potentially relevant to anticipated or ongoing litigation, regulatory investigations, or internal audits. This process overrides standard retention and disposal schedules.
- The Legal Department is responsible for initiating, managing, and releasing legal holds.
- IT and Data Owners are responsible for assisting the Legal Department in identifying, locating, and preserving the relevant data in a forensically sound manner.
- Custodians (employees whose data may be relevant) are formally notified of their obligations under a legal hold.

- All legal hold activities, including issuance, scope, custodians, data sources, and release, must be meticulously documented.
- *Use Case (Legal Hold for Regulatory Inquiry):* World Bank's Compliance department receives a formal inquiry from a financial regulator regarding a series of international development project financing transactions conducted between 2018 and 2020. The Legal department immediately issues a legal hold notice to all current and former employees involved in these projects, as well as to IT for the preservation of all relevant email communications, transaction records, project files, and meeting minutes from the specified period. Standard deletion of these records is suspended until the legal hold is formally lifted by the Legal department.
- **Monitoring, Auditing, and Enforcement:**
 - Regular audits (internal and/or external) must be conducted to verify compliance with this Data Retention Policy and the associated Data Retention Schedule.
 - System logs related to data access, modification, and deletion are monitored to detect any unauthorized activities or deviations from policy.
 - Non-compliance with this policy will be subject to disciplinary action, as outlined in the Security Code of Conduct.
- **Training and Awareness:**
 - All World Bank employees must receive training on this Data Retention Policy and their specific responsibilities regarding the handling, retention, and disposal of Bank data.

Framework Alignment

This Data Retention Policy is designed to align with:

- **ISO 15489 (Records Management):** Incorporates principles for the creation, capture, maintenance, and disposal of records.
- **GDPR (General Data Protection Regulation):** Particularly Article 5 principles of purpose limitation, data minimization, and storage limitation.
- **SEC Rule 17a-3 and 17a-4 (for broker-dealers, principles adaptable for banking):** Provides specific guidance on record types and retention periods for financial institutions. While World Bank may not be a broker-dealer, these rules offer a benchmark for financial recordkeeping.
- **FINRA Rules (e.g., Rule 4511):** Complements SEC rules regarding books and records for member firms.

- **FFIEC Guidance:** The FFIEC emphasizes robust records management as part of overall IT governance and operational risk management for financial institutions.
- **NIST Publications:** Guidance on media sanitization (NIST SP 800-88) is integral to the secure disposal aspect of this policy.

Real-World Example: Managing Email Retention

World Bank implements a policy for email retention:

- **Data Classification:** Emails are classified based on their content. General correspondence may be "Internal Use Only," while emails containing sensitive project financials or client PII are "Confidential" or "Restricted."
- **Retention Schedule:**
 - General business emails: Retained for 5 years in an active, searchable archive.
 - Emails related to specific financial transactions or legal matters: Linked to the relevant transaction/case file and retained according to that record's schedule (which might be longer, e.g., 7-10 years or indefinitely if under legal hold).
 - Transient/personal emails with no business value: Users are encouraged to delete promptly; automated cleanup may apply after a shorter period (e.g., 90 days) if not explicitly saved to a business record.
- **Archiving:** After 2 years, general business emails are moved from primary mailboxes to a secure, indexed, and searchable long-term archive. Access to the archive is controlled and logged.
- **Disposal:** After the 5-year retention period (unless subject to a legal hold), general business emails are flagged for secure deletion from the archive. The deletion process is logged.
- **Legal Hold:** If an employee is a custodian in a legal matter, their entire mailbox (or specific relevant folders/date ranges) is placed on legal hold, preventing any automated or manual deletion.

Table: World Bank Data Retention Schedule (Excerpt)

Data Category	Data Owner Department(s)	Specific Data Type/Examples	Key Legal/Regulatory Citation(s) (Illustrative)	Retention Period (Minimum)	Storage (Active/Archive)	Secure Disposal Method (Post- Retention & No Hold)

Customer Account & Transaction Records	Retail Banking, Treasury	Account opening docs, KYC/CDD records, transaction confirmations, statements, loan agreements	AML/CFT Regs, Local Banking Acts, SEC 17a-4 (principles)	7 years after account closure/transaction	Active (2 yrs), Archive (5 yrs)	Purge/Destroy (NIST 800-88)
Internal Financial & Audit Records	Finance, Internal Audit	General ledger, financial statements, audit reports, regulatory filings	SOX (principles), Local Corp. Law	Financial Statements: Permanent; Audit Reports: 10 years	Active (3 yrs), Archive (7+ yrs/Perm)	Purge/Destroy (for non-permanent)
Electronic Communications (Email/IM)	All Departments	Business-related correspondence, project communications, internal memos	FINRA Rules (principles), GDPR	5 years (general); longer if case-specific	Active (2 yrs), Archive (3 yrs)	Secure Deletion (overwrite)
Employee Records	Human Resources	Employment contracts, performance reviews, payroll, benefits information	Local Labor Laws, GDPR	Duration of employment + 7 years	Active/Secure HR Archive	Secure Shredding (physical), Purge (digital)
Security Logs (Critical Systems)	IT Security, IT Operations	Firewall logs, IDS/IPS logs, critical server access logs, authentication logs	PCI DSS (Req 10 principles), FFIEC	1 year (3 months readily accessible)	SIEM (Active), Secure Log Archive	Secure Deletion
Project Documentation (Development Finance)	Project Finance Departments	Project proposals, feasibility studies, environmental impact assessments, loan disbursement records	World Bank Operational Policies	Life of project + 10 years	Active/Secure Project Archive	Review for historical value, then Secure Deletion

- Value of Table:** This Data Retention Schedule is the operational core of the Data Retention Policy. For World Bank, an institution handling vast amounts of diverse and often highly sensitive data across numerous jurisdictions, this schedule provides indispensable clarity and direction. It ensures that:
 - Compliance:** The Bank meets complex and varied legal and regulatory obligations globally (e.g., financial record-keeping like SEC 17a-4 , data privacy like GDPR).

2. **Risk Management:** The risk of retaining data unnecessarily (increasing attack surface, discovery costs) or disposing of it prematurely (legal/regulatory penalties, loss of evidence) is minimized.
3. **Operational Efficiency:** Departments have clear guidance, reducing ambiguity and improving consistency in records management.
4. **Cost Optimization:** Storage costs are managed by ensuring data is not kept indefinitely without justification and by utilizing appropriate archiving solutions.
5. **Auditability:** The schedule provides a clear basis for internal and external audits of the Bank's records management practices. This structured approach is fundamental for demonstrating due diligence and responsible data governance, which are paramount for an institution of World Bank's stature.