Policy on Records Management

Table of Contents

1. Introduction

Records provide evidence of the BSTDB's communications, decisions and actions and form the basis of its institutional memory. The Bank's processes and activities are dependent for their operational efficiency and regularity on good records management, and its internal governance includes many explicit references to record-keeping obligations[1]. To ensure compliance with these obligations it is necessary to have in place provisions to ensure records are properly managed in line with internationally accepted best practice and standards, and that staff understand what is expected of them with regard to the records they generate and handle in the course of their work.

Building on the requirements of related internal governance on issues such as protection of Personal Data and public access to information, and by further developing the advanced technical platforms already in place, the Bank has the possibility to provide, in its approach to records management, an exemplary model of good information governance among the IFI community.

Overall responsibility for overseeing the management of the Bank's records lies with the Secretary General, with records and related information management tasks defined as falling under the remit of the Administration Division in the policy document '01.16 Organizational Structure'[2]. This is also in line with internationally accepted best practice in records management, which prescribes that information management activities are overseen by 'a senior executive (or a person of comparable authority)'[3].

2. Purpose, Objectives and Scope

2.1 Purpose

The purpose of creating this policy is to:

- Put in place a policy framework for records management that provides a foundation for the development of implementing procedures and actions;
- Clarify accountability for and responsibilities concerning records management;
- Establish overarching principles, based on internationally accepted best practice and standards, governing what types of information should be captured as records, how and by whom records should be captured, classified and accessed, and the manner in which they should be managed throughout their lifecycle;
- Promote further automation/digitalisation of the Bank's business processes, in line with the Bank's strategic goals and objectives, with the aim of increasing efficiency and reducing the use of paper to a minimum;
- Reinforce to staff the importance of records management to the Bank, both operationally and strategically.

[1] Some examples include: the detailed list of records presented in the Operations Manual; references to FATF minimum retention periods in the Anti-Fraud Policy, and the emphasis on record deletion times in the Policy on Personal Data Protection.
[2] 01.16 Organizational Structure – last updated 29 September 2007 by BoD Decision 0792
[3] The first of ARMA's Generally Accepted Record-keeping Principles, on Accountability, prescribes that information management is overseen by '*a senior executive (or a person of comparable authority)*'.

2.2 Objectives

The key objectives of this policy are to ensure that:

- The Bank can present itself as an exemplary model of good information governance;
- Accountability for and responsibilities concerning records management are clearly defined;
- Staff understand their obligations concerning records management;
- Records are properly captured, classified and stored;
- Records are managed in a way that guarantees their integrity and authenticity over time;
- Records, particularly those containing confidential information and Personal Data, are adequately protected against unauthorized access;
- Records exist in formats and are stored in a manner that supports the mitigation of operational risk and guarantees compliance and/or alignment with the provisions of the Bank's governance and all relevant internal and any applicable external legal and regulatory requirements and IFI best practice;
- Records are readily available for access by authorized staff and stakeholders;
- Records are retained for agreed periods of time and are disposed of (i.e. erased, or processed for long-term preservation) in a timely manner, in particular to satisfy policy requirements concerning storage limitation of Personal Data;
- Records management is integrated into business processes; and
- To the extent possible and practical, records are kept in digital format only.

2.3 Scope

This Policy is applicable to Bank Officials and Staff Members. Within this Policy, the term 'staff' is used to refer to both these categories of person.

It is also applicable to any other individual engaged by the Bank, to the extent set out in their Terms of Reference or contracts, as the case may be, if such documents define record-keeping obligations.

It is applicable to Board Officials only in that it concerns how records of the Bank's activities, including activities of the Boards, are managed. It does not impose any record-keeping obligations on Board Officials.

It applies to all records created or received by the Bank in the course of its operations and activities, regardless of their format.

Private records belonging to an individual personnel member or any third party that have not been received, created or used in the conduct of the Bank's business fall outside of the scope of this Policy.

3. Terms & Abbreviations

3.1 Terms

For the purposes of this Policy, the following definitions shall apply:

Active records: records used in the course of the Bank's ongoing business operations.

Capture: the insertion of a document or other information asset into an official electronic repository by combining a unique identifier and metadata[4].

Classification (of records[5]): act of classifying records according to the business functions and activities that give rise to their creation.

Disposition: agreed actions undertaken of records at the end of their approved retention period (i.e. erasure or preservation, with specific conditions, as appropriate).

Inactive records: records that have completed their active phase.

Personal data: has the meaning ascribed to it in the BSTDB's Policy on the Protection of Personal Data.

Physical Archives: inactive physical (i.e. paper or analogue) records being kept in storage until the expiry of their retention period, as well as physical records flagged for permanent preservation on account of their long-term value and contribution to the institutional memory of the BSTDB.

Records: finalized documents or other information assets, in whatever format, that, in relation to the execution or support of the Bank's activities, provide evidence of activities, transactions, decisions and actions taken, and/or are likely to require action, follow-up, or reply. For the avoidance of any doubt, any and all 'records' of the Bank, as herein defined, are covered by the immunity enshrined in Article 47 of the Agreement for Establishment of the BSTDB, yet the immunity coverage of such provision can extend to information and equipment that might not necessarily or obviously be captured by the definition of 'records' in this Policy. There is no intent, express or implied by BSTDB to waive or constrain in any sense through this definition of 'records' the extent and broad spectrum of the absolute immunity coverage enshrined in such Article.

Records Management Coordinator: each Department/Unit's designated main point of contact on records management issues.

Vital records: records containing information critical to recreate the Bank's legal and financial status and to preserve the rights and obligations of shareholders, employees, customers and investors, during or immediately following a crisis.

3.2 Abbreviations

The following abbreviations are used in this Policy:

Abbreviation	Full Wording of Abbreviation:
DCR	Compliance and Operational Risk Management Office
DGC	Office of the General Counsel
DIA	Internal Audit Department
DIT	Department for Information Technologies

[4] See ISO 15489-1:2016, point 9.3.

[5] *Not to be confused with Information Security Classifications, which concern the level of protection given to information*

DPO	Data Protection Officer
RM	Records Management

4. Roles and Responsibilities

The following Business Units and Positions are responsible for the corresponding tasks:

- **Secretary General**
  - has overall accountability for records management at the Bank;
  - plans, budgets and allocates, as appropriate, necessary staff and technical resources.

- **DIT**
  - puts in place and configures information systems with features that support the essential records management principles defined in this Policy;
  - provides technical support and guidance on the capture of records in information systems and the use integration options, where appropriate, to facilitate and automate capture and to incorporate records management into business processes;
  - provides technical support regarding the use of e-signatures that may feature in records;
  - responsible for safeguarding records.

- **Records Officer (DIT)**
  - maintains and implements a BSTDB 'Records Classification and Retention Plan', in consultation with DGC, DIA, DCR and the DPO;
  - ensures records are securely erased/destroyed in a timely manner, as per the 'Records Classification and Retention Plan', and makes sure erasure/destruction is put on hold, if so instructed, as appropriate for audit, compliance, legal or other reasons;
  - provides Departments/Units, in particular via liaison with their RM Coordinators, with guidance, training and support regarding the management of their records and interpretation of this Policy and its implementing procedure(s).

- **DGC**
  - consulted by the Records Officer on defining retention periods, in particular regarding legal requirements;
  - provides advice on the evidentiary value of records and the validity of their format;
  - assists the Records Officer in determining the type of records where various types of e-signature can and should be efficiently utilized, where demanded by the evolving needs of the Bank, to ensure that records bearing such signatures constitute valid records in whatever forum they might need to be presented;
- **DIA**
  - consulted by the Records Officer on defining minimum retention periods, in particular regarding internal/external auditing requirements;
  - independently audits the Bank's Records Management systems and processes in place, including physical security and access for records held within or outside the Bank, to assess their effectiveness and efficiency;
  - reviews from an audit/control perspective, any proposed usage of e-signatures in records, embedded in the Bank's procedures or systems, in reference to section 5.5.3 Compliance below;
  - in accordance with the Internal Audit Charter, is granted access to all records by default.

- **DCR/DPO**
  - consulted by the Records Officer on defining minimum retention periods, in particular regarding compliance issues;
  - (in capacity as DPO) consulted by the Records Officer on defining maximum retention periods (storage limitation) for records that contain Personal Data, and on the handling of such records;
  - in accordance with the Charter of the Compliance and Risk Management Office, on every compliance and operational risk management assignment, the accountable management is expected to allow unrestricted right of access to DCR staff to any records or files necessary to enable it to carry out its responsibilities, with the exception of those of the Internal Audit Department (DIA);
  - (in capacity as DPO) granted access, as needed, to all records necessary to address data subjects' requests and to investigate Personal Data breaches, in line with the Bank's rules on Personal Data Protection.

- **Department/Unit Heads**
  - responsible for the effective and well-coordinated management of records throughout their Departments/Units.

- **Records Management Coordinators** *(designated staff member from each Department Unit)*
  - act as the Department/Unit's main point of contact with the Records Officer on records issues, and with DIT on the related use of information systems.
  - following guidance provided by the Records Officer, provide information, support and instruction to the staff of the Department/Unit to ensure that the provisions and objectives of this Policy and its implementing procedure(s) are observed.

- **All BSTDB staff**
  - responsible for documenting their activities and decisions and for ensuring, in the performance of their duties, that the records they generate or receive are properly captured and classified, in accordance with the Bank's rules.

5. Policy

5.1 Accountability and responsibility

Overall accountability for records management at the Bank lies with the Secretary General.

The Heads of each Department/Unit are responsible for the effective and well-coordinated management of records throughout their Departments/Units.

All staff are responsible for documenting their activities and decisions and for ensuring, in the performance of their duties for BSTDB, that the records they generate or receive are properly captured and classified. Staff Members shall be provided with necessary guidance and training, by the RM Coordinator of their Department/Unit and the Records Officer, to ensure they understand and can adequately fulfil this obligation (see Section 5.9 – Training and awareness-raising below).

5.2 Coordination

The Head of each Department/Unit shall designate from their staff a 'Records Management Coordinator' (RM Coordinator) who will be the Department/Unit's main point of contact with the Records Officer on records management issues, and with DIT on the related use of information systems. Following guidance provided by the Records Officer, the RM Coordinators shall provide information, support and instruction to the staff of the Department/Unit to ensure that the provisions and objectives of this Policy and its implementing procedure(s) are observed.

5.3 Ownership

BSTDB records are BSTDB property and shall not be used for personal or private purposes.

Upon termination of service in BSTDB, personnel may not retain or remove from BSTDB any records or archives, except for copies of public documents and any records directly related to the terms and conditions of their service.

5.4 Identification, capture and classification

5.4.1 Identification

Records are *finalised* documents or other information assets, in whatever format, that, in relation to the execution or support of the Bank's activities:

- *provide evidence of activities, transactions, decisions and actions taken, and/or*
- *are likely to require action, follow-up, or reply.*

Information that has been received and used as reference, copies of records or documents kept only for personal convenience, and drafts, other than those that provide valuable evidence of the decision-making process and exist as supporting documents to finalised records[6], shall not be managed as records, though they shall remain covered by the immunity of Article 47 of the Agreement for Establishment of BSTDB.

More specific guidance on what should and should not be considered a record shall be further elaborated in this Policy's implementing procedures.

The Bank's 'Records Classification and Retention Plan' (*see Section 5.5.5 Retention and Disposition below*), in presenting a comprehensive list of all categories of record created and managed by the Bank, shall also assist staff in identifying records.

5.4.2 Capture and records classification

Records shall be captured and managed in a records management system that supports the records management principles and objectives outlined in this Policy and its implementing procedure(s). DIT shall ensure such systems are in place, are suitably configured, and are properly maintained and upgraded.

Records can be introduced into a records management system in a variety of ways, depending on the format of the record and how it has been created or received. DIT shall provide technical support and guidance on this matter, using integration options, and, where appropriate, to facilitate and automate the capture and to incorporate records management into business processes.

[6] For example, draft documents formally submitted to the Management Committee for their consideration

When saved into a records management system, records shall be assigned a records classification in accordance with the Bank's 'Records Classification and Retention Plan' (*see Section 5.5.5 – Retention and Disposition below*). DIT shall support this process by configuring information systems so that, wherever possible, accurate records classifications are automatically applied to saved content.

Personnel should not file private records in records management systems. Any private records, including emails, kept in these systems will be subject to the Bank's applicable rules on the use of its information systems.

5.5 Essential principles

Organisational and technical measures and controls, to be elaborated in this Policy's implementing procedure(s), shall be in place to ensure that records are managed in accordance with the essential principles described in this section. These principles are derived from internationally accepted best practice and standards[7].

5.5.1 Integrity

The integrity of records shall be maintained by ensuring they are protected against unauthorized modification or erasure, so that they remain authentic and reliable.

Records identified as being 'vital' shall be protected from potential destruction or loss with additional measures concerning protective storage and dispersal, as per the Bank's Business Continuity Plan.

5.5.2 Protection

Records containing confidential business information and Personal Data shall be protected against unauthorized access. Appropriate controls shall be in place to protect records through their entire lifecycle, from their creation until their eventual disposition. These controls shall include the application of Information Security Classification markings, to be defined in a dedicated policy.

5.5.3 Compliance

Records shall be managed and retained in a manner that supports the mitigation of operational risk and guarantees compliance and/or alignment with relevant legal and regulatory requirements, industry-specific standards, IFI best practice, audit recommendations, and the provisions of the Bank's internal governance.

DGC, DIA, DCR and the DPO shall provide advice and instruction regarding interpretation of the above, in particular concerning the evidentiary validity of records and their retention periods and disposition.

The Records Officer, with the advice of DGC, technical support of DIT, and independent audit review of DIA, shall determine for which type of records e-signatures can and should be efficiently utilized, where strictly necessary, to ensure that records bearing such signatures constitute valid records in whatever forum they might need to be presented.

[7] Specifically: ARMA's Generally Accepted Record-keeping Principles; ISO 15489-1:2016 - Information and documentation — Records management — Part 1: Concepts and principles

5.5.4 Availability and access

Staff members shall be able to securely and easily access, from any location, records that contain information they need in order to carry out their duties.

In accordance with the Internal Audit Charter, DIA shall be granted access to all records by default.
In accordance with the Charter of the Compliance and Risk Management Office, on every compliance and operational risk management assignment, the accountable management is expected to allow unrestricted right of access to DCR staff to any records or files necessary to enable it to carry out its responsibilities, with the exception of those of the Internal Audit Department (DIA). Also, for data protection purposes, DCR shall be granted access, in capacity as DPO, to all records necessary to address data subjects' requests and to investigate Personal Data breaches.

5.5.5 Retention and disposition

The Records Officer shall maintain and update a 'Records Classification and Retention Plan' describing all categories of record created and managed by the Bank, the required retention period for each, and the required disposition (i.e., whether records should be erased or preserved, with specific conditions as appropriate) to satisfy legal, regulatory, fiscal, operational, audit and historical requirements.

Retention periods shall be defined primarily in consultation with DGC, but also with input where necessary from DIA, DCR and the DPO, to ensure records are retained for, at a minimum, the period of time in which there could be a need to consult them, while taking into account the principle of storage limitation with regard to records containing Personal Data.

Records shall not be erased/destroyed unless destruction is approved in the 'Records Classification and Retention Plan', and they shall be erased/destroyed in a secure manner, to be elaborated in this Policy's implementing procedure(s).

If a need arises to put a scheduled destruction of records on hold, thus extending the retention period in exceptional and justified cases, this shall be formally communicated to the Records Officer, informing the Secretary General. The necessity for the hold shall subsequently be reviewed every six months.

Controls shall be put in place to ensure the long-term or permanent preservation of records identified as having historical value and to support policy requirements concerning public access to documents. The process for declassifying historical records shall be covered in an implementing procedure to this Policy.

5.6 Digital transformation

The BSTDB is committed to its vision to be transformed into a paperless bank, reducing dramatically the paper load produced during its daily activities. In this context, the Bank will adopt the following key principles:

- The Bank shall endeavour to digitalize business processes that generate records, to improve efficiency and to minimize the generation and storage of physical (paper) records. Furthermore, providing that the identity of approvers can be verified and is auditable, workflow processes comprised of approval steps in information systems shall be preferred over processes that generate document records.

- The Bank shall use e-signatures to the appropriate extent with the aim of eliminating the inefficiencies associated with physical signatures (the need to print documents, obtaining

signatures in person, scanning documents, etc.). Such e-signatures must comply with an agreed and widely recognized framework. As described in *section 5.5.3 - Compliance* above, the Records Officer, with the advice of DGC, technical support of DIT, and independent audit review of DIA, shall determine for which type of records e-signatures can and should be efficiently utilized, where strictly necessary, to ensure that records bearing such signatures constitute valid records in whatever forum they might need to be presented. DIT shall be responsible for monitoring and safeguarding the signed records.

5.7 Physical records

Physical records shall be digitized, with the hard copies being kept only where strictly necessary. Physical records kept in originating offices, once inactive, shall be transferred to the Bank's central archiving facilities for further processing, in accordance with this Policy's implementing procedure(s).

The Bank's 'Physical Archives' shall thus be comprised of physical inactive records that are being kept in storage until the expiry of their retention period and ultimately their destruction, as well as physical records flagged for permanent preservation on account of them having long-term value and contributing to the institutional memory of the BSTDB.

5.8 Resource requirements

The Bank, via the Secretary General, shall plan, budget and allocate, as appropriate, necessary staff and technical resources to ensure that records can be properly managed in accordance with this Policy and its implementing procedure(s).

5.9 Training and awareness-raising

Staff shall be provided with regular training on records management, along with guidance materials including a relevant Handbook providing a user-friendly summary of how the records management principles presented in this Policy and its implementing procedure(s) should be applied in practice.

5.10 Implementation and transparency

This policy shall be supported by implementing procedures and, where appropriate, working instructions covering, at a minimum:

- Application and periodic update of a 'Records Classification and Retention Plan'
- Declassification of historical records
- Transfer of physical records (internally, and to external storage)
- Digitization standards (in particular regarding scanning)
- Use of digital signatures in records
- Proof of destruction of records, where that is necessary

Documents concerning implementation of records management at the Bank, including this Policy, shall be presented in a manner that ensures structure, processes, and activities are apparent, understandable, and reasonably available to legitimately interested parties.

In particular, and as described in section *5.9 Training and awareness-raising* above, a Handbook providing a user-friendly summary of how the records management principles presented in this Policy and its implementing procedure(s) should be applied in practice shall be created and made available to personnel.

6. References

- ISO 15489-1:2016 - Information and documentation — Records management — Part 1: Concepts and principles
- ARMA's Generally Accepted Record-keeping Principles ((https://www.arma.org/page/principles)