Information Classification Policy

- **Purpose:** This policy establishes the World Bank's framework for classifying its information assets based on their sensitivity, value, criticality, and any legal or regulatory requirements. The primary objective is to ensure that all WDB information is protected by security controls appropriate to its classification level throughout its lifecycle (creation, storage, processing, transmission, and disposal).
- **Scope:** This policy applies to all World Bank information assets, regardless of their form (e.g., digital, paper, audio, video), location (e.g., on-premises, cloud, third-party sites), or the media on which they are stored or processed. It applies to all WDB personnel (employees and contractors) and any third parties who are authorized to access or handle WDB information.
- **Roles and Responsibilities:**
    - **Data Owners (Information Asset Owners - IAOs):** As defined in Section A.2, IAOs are primarily responsible for:
        - Assigning an initial classification level to the information assets under their stewardship, in accordance with this policy.
        - Periodically reviewing and, if necessary, re-classifying these assets.
        - Defining access rights and specific handling procedures for their assets, consistent with the assigned classification.
    - **Data Custodians (typically IT personnel):** Responsible for implementing and maintaining the technical security controls (e.g., access controls, encryption, logging) required to protect information assets according to their assigned classification level.
    - **Data Users (all WDB personnel and authorized third parties):** Responsible for understanding and adhering to the handling requirements associated with the classification level of any WDB information they access or use.
- **Classification Levels:** The World Bank employs a four-tier information classification scheme to provide sufficient granularity for its diverse information assets. The impact levels (Critical, High, Moderate, Low) for Confidentiality, Integrity, and Availability are key determinants in assigning these classifications.
    - **Level 4: Highly Restricted**
        - **Description:** Information of the utmost sensitivity. Unauthorized disclosure, modification, or unavailability could cause exceptionally grave damage to the World Bank, its clients, member countries, or international financial stability. This includes potential loss of life, severe

diplomatic repercussions, systemic financial crisis, or compromise of national security interests related to WDB operations.

- **Examples:** Strategic plans for state-level financial interventions, master cryptographic keys for systemic payment systems, highly sensitive intelligence data related to economic stability, information under strict governmental secrecy agreements.
- **Impact Profile:** Critical Confidentiality, Critical Integrity, High/Critical Availability.

- **Level 3: Restricted**
  - **Description:** Sensitive information requiring stringent protection. Unauthorized disclosure, modification, or unavailability could cause serious damage to the World Bank's operations, finances, reputation, or result in significant legal/regulatory penalties. This includes breaches of privacy for large numbers of individuals or highly sensitive personal data.
  - **Examples:** Personally Identifiable Information (PII) of clients and employees (e.g., financial account details, health records if applicable, detailed personnel files), detailed institutional financial records not yet public, pre-release market-sensitive economic reports, critical system passwords and configurations, proprietary risk models, sensitive legal case files, detailed internal audit findings.
  - **Impact Profile:** High Confidentiality, High Integrity, Moderate/High Availability.
- **Level 2: Confidential (Internal)**
  - **Description:** Information intended primarily for internal use within the World Bank. Unauthorized disclosure could cause moderate damage, operational disruption, minor financial loss, or embarrassment to the Bank.
  - **Examples:** Internal operational procedures, draft reports and policy documents not yet approved for wider circulation, non-sensitive project plans and data, internal staff directories with limited PII, minutes of routine internal meetings, most inter-office correspondence.
  - **Impact Profile:** Moderate Confidentiality, Moderate Integrity, Moderate Availability.
- **Level 1: Public**
  - **Description:** Information that has been explicitly approved for release to the public or is already in the public domain. Unauthorized modification

could cause minor reputational damage or inconvenience, but disclosure carries no confidentiality risk.

        - **Examples:** Published annual reports, press releases, publicly available research papers, general information on the WDB website, marketing materials, job vacancy announcements.
        - **Impact Profile:** Low Confidentiality, Low/Moderate Integrity (ensuring accuracy of public information is still important), Low/Medium Availability.

- **Classification Process:**
    - Information Asset Owners (IAOs) are responsible for initially classifying information assets at the time of their creation or acquisition.
    - Classification decisions must be based on an assessment of the information's sensitivity, criticality, and any applicable legal or regulatory requirements, using the criteria defined in this policy.
    - Classifications must be reviewed periodically (e.g., annually or when significant changes occur to the asset or its context) by the IAO to ensure they remain appropriate.
    - If an information asset is aggregated from multiple sources with different classifications, the aggregated asset generally inherits the highest classification level of its components.
- **Handling Requirements per Level:** Specific, mandatory handling procedures are defined for each classification level. These requirements address the entire information lifecycle. The table below provides a summary. More detailed procedures may be documented in supporting standards and guidelines.
- **Labeling:** Information assets, where practical, should be labeled (digitally or physically) with their classification level to inform users of handling requirements.
- **Appendix A: Examples of Data Types and Default Classifications:** An appendix to this policy provides a non-exhaustive list of common WDB data types and their presumed default classification levels to assist IAOs in the classification process (e.g., all employee Social Security Numbers are Level 3: Restricted).

Key Table: Data Classification Levels, Criteria, and Handling Requirements

Level	Description	Examples for WDB	Confidentiality Impact	Integrity Impact	Availability Impact	Key Handling Requirements (Summary)
L1: Public	Information approved for public release.	Published annual reports, press releases, general website information.	Low	Low/Moderate	Low/Medium	No access restrictions for viewing. Protect against unauthorized modification. Ensure public availability through appropriate channels.
L2: Confidential (Internal)	For internal WDB use. Unauthorized disclosure could cause moderate harm.	Internal memos, operational procedures, non-sensitive project data, staff directories with limited contact info.	Moderate	Moderate	Moderate	Access restricted to WDB personnel and authorized contractors with a legitimate business need. Encrypt when stored on mobile devices or transmitted over untrusted networks. Dispose of securely (e.g., shredding, secure wipe).
L3: Restricted	Sensitive data. Unauthorized disclosure could cause serious harm.	Client PII, employee PII, detailed financial records, pre-release economic data, system credentials.	High	High	Moderate/High	Strict need-to-know access controls (least privilege). Strong encryption required at rest and in transit. Prohibit storage on unapproved personal devices or insecure public cloud services. Secure authenticated transmission methods. Access logs monitored. Secure, verified disposal.
L4: Highly Restricted	Extremely sensitive. Unauthorized disclosure could cause exceptionally grave harm.	State-level financial intervention plans, systemic cryptographic keys, national security related intelligence.	Critical	Critical	High/Critical	Access strictly limited to named, authorized individuals with explicit approval. Often requires segregated networks/systems. Hardware-based encryption preferred. Multi-person control for critical operations. No external network connectivity unless explicitly and securely engineered.