

# Identity Management Rules and Procedures

## 1.1. Introduction

**Purpose:** The purpose of this document is to establish clear, comprehensive, and enforceable rules and procedures for managing digital identities and controlling access to World Bank's information systems, applications, and data resources. Effective identity and access management (IAM) is paramount to safeguarding the Bank's assets, ensuring the confidentiality, integrity, and availability of information, maintaining customer trust, achieving regulatory compliance, and supporting operational efficiency.

**Scope:** These Identity Management Rules and Procedures apply to all individuals who require access to World Bank's information technology environment. This includes, but is not limited to, full-time and part-time employees, contractors, consultants, third-party vendors, temporary staff, and any automated systems or services that interact with the Bank's IT resources. The scope covers the entire lifecycle of an identity, from initial creation and provisioning through to modification, review, and eventual de-provisioning.

**Audience:** This document is intended for all personnel of World Bank. Specific sections will be of particular relevance to IT staff responsible for administering IAM systems, the Cybersecurity team responsible for oversight and policy enforcement, the Human Resources (HR) department involved in personnel lifecycle management, and managers responsible for authorizing and reviewing access for their team members. All users are expected to understand and adhere to the responsibilities outlined herein.

**Regulatory Context:** The procedures detailed within this document are formulated in strict adherence to the prevailing regulatory landscape governing financial institutions. Key considerations include guidance from the Federal Financial Institutions Examination Council (FFIEC), specifically concerning authentication and access to financial institution services and systems. Furthermore, these procedures align with the requirements of the Gramm-Leach-Bliley Act (GLBA) for protecting customer financial information and draw upon best-practice principles from established cybersecurity frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and ISO 27001. Financial institutions operate under intense regulatory scrutiny, where robust IAM practices are not merely recommended but mandated. FFIEC guidance, for instance, explicitly calls for strong authentication mechanisms and diligent access management protocols. The GLBA's mandate to protect sensitive customer data inherently relies on effective controls over who can access this information. Frameworks like NIST CSF and ISO 27001 provide structured approaches for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS), within which IAM serves as a critical foundational pillar. The meticulous application of these IAM rules and procedures is therefore essential for World Bank to meet its legal and regulatory obligations and to protect its reputation and assets.

## **1.2. User Identification and Authentication Requirements**

**1.2.1. Unique User Identification:** Every individual granted access to World Bank systems must be assigned a unique User Identifier (User ID). This User ID will serve as the primary means of identifying the user within the Bank's IT environment. The sharing of User IDs between individuals is strictly prohibited under all circumstances. *Rationale:* Unique User IDs are fundamental for establishing individual accountability. They ensure that all actions performed on the Bank's systems can be traced back to a specific person, which is crucial for security monitoring, incident investigation, and audit purposes.

**1.2.2. Password Complexity and Strength:** All passwords used to access World Bank systems must adhere to the Bank's Password Policy. This policy mandates specific requirements for password complexity, including minimum length (e.g., 12 characters), the use of a combination of character types (uppercase letters, lowercase letters, numbers, and special symbols), and restrictions against using easily guessable information. Further details are available in the "Security Code of Conduct" or the standalone "Password Policy" document. *Rationale:* Strong passwords form the first line of defense for "something you know" authentication, making it significantly harder for unauthorized individuals to guess or crack credentials.

**1.2.3. Multi-Factor Authentication (MFA) Enforcement:** Multi-Factor Authentication (MFA) is mandatory for all forms of remote access to World Bank's network and systems. Furthermore, MFA must be employed for accessing sensitive systems, which include but are not limited to core banking platforms, customer data repositories, financial reporting systems, SWIFT interfaces, and any system housing critical or regulated data. All privileged accounts (e.g., administrator accounts, service accounts with elevated permissions) must also utilize MFA. *Rationale:* MFA provides a significant additional layer of security by requiring users to present multiple types of credentials. This drastically reduces the risk of unauthorized access even if one factor (like a password) is compromised. FFIEC guidance strongly emphasizes the use of MFA for financial institutions. *Use Case:* A Relationship Manager attempting to access the Customer Relationship Management (CRM) system from their home office must first enter their unique username and password. Following successful primary authentication, they will be prompted to provide a one-time code generated by an authenticator application on their Bank-issued mobile device. Only upon successful validation of both factors will access be granted.

**1.2.4. Authentication Factors:** For MFA to be effective, it must utilize at least two distinct authentication factors. These factors are categorized as: \* Something you know (e.g., password, PIN). \* Something you have (e.g., hardware token, software token on a mobile app, smart card). \* Something you are (e.g., fingerprint, facial recognition, voiceprint). *Rationale:* Using diverse factors ensures that the compromise of a single factor does not lead to a system breach.

**1.2.5. Biometric Authentication:** Where biometric authentication methods are implemented by World Bank (e.g., fingerprint scanners for access to secure physical locations like data centers, or facial recognition for unlocking specific corporate devices), these methods must meet stringent Bank-approved standards for accuracy, reliability, and resistance to spoofing. The storage and processing of biometric data must also comply with all applicable privacy and security regulations. *Rationale:* Biometrics, when implemented correctly, can offer a convenient and strong authentication factor. However, their unique nature requires careful management to prevent compromise and ensure user privacy.

**1.2.6. Passwordless Authentication Exploration:** World Bank is committed to continuously enhancing its security posture and user experience. As such, the Bank will actively explore, pilot, and consider the adoption of passwordless authentication methods where feasible, secure, and aligned with business needs. Examples include FIDO2-compliant security keys or the integration of robust biometric authentication directly with enterprise systems. *Rationale:* Passwordless methods aim to eliminate the risks associated with passwords (e.g., weak passwords, credential stuffing, phishing) and can improve user convenience. This proactive approach aligns with emerging best practices in identity management.

The evolution of IAM is moving towards models like Zero Trust, which emphasizes "trust no one, verify everything," and continuous authentication. This signifies a fundamental shift from traditional perimeter-based security, which often assumes trust once a user is inside the network, to an identity-centric security model where trust is never assumed and verification is ongoing. For World Bank, this implies that IAM policies and procedures must be dynamic and adaptive. It's not sufficient to simply grant access based on an initial authentication; the Bank must move towards continuously validating that access, potentially through context-aware adaptive MFA, behavioral biometrics, or other advanced techniques. This necessitates more sophisticated monitoring and response capabilities tied directly to identity events, ensuring that access remains appropriate throughout a user's session and lifecycle.

### **1.3. Role-Based Access Control (RBAC) Framework**

**1.3.1. RBAC Implementation:** Access to World Bank's systems, applications, and data will be granted based on a Role-Based Access Control (RBAC) model. Predefined roles will be established, aligning with specific job responsibilities, functions, and duties within the Bank. *Rationale:* RBAC simplifies the administration of user permissions, enhances security by ensuring access is tied to job function rather than individual discretion, supports regulatory compliance by providing a clear framework for access rights, and reduces the risk of excessive privileges.

**1.3.2. Role Definition and Maintenance:** The definition of roles and their associated access permissions is a collaborative effort. Business Unit Heads, in conjunction with the Human Resources department and the IT Cybersecurity team, are responsible for accurately defining these roles. These roles, and the permissions they entail, must be formally documented and reviewed at least annually, or more frequently if significant changes occur in job functions,

organizational structure, or system functionalities. *Rationale:* Roles must accurately reflect current business needs and job responsibilities to be effective. Regular reviews prevent roles from becoming outdated and granting inappropriate access.

**1.3.3. Segregation of Duties (SoD):** The RBAC framework must be implemented in a manner that inherently supports and enforces the principle of Segregation of Duties (SoD). This is critical for preventing conflicts of interest, fraud, and unauthorized actions. For critical financial transaction processes or sensitive system administration tasks, the completion of a process will require actions from individuals in two or more distinct roles. *Rationale:* SoD is a fundamental internal control mechanism that reduces the risk of errors and malicious activities by ensuring no single individual has control over all phases of a critical transaction or process. *Example:* Within the wire transfer system, a user assigned the "Wire Initiation" role can create a wire transfer request, but a different user with the "Wire Approval" role must authorize it before it can be processed. No single user will possess both roles for high-value transactions.

**1.3.4. Access Inheritance:** Users will primarily inherit their access permissions based on the role(s) assigned to them. The direct assignment of permissions to an individual user, outside of their formally defined role(s), is strongly discouraged. Such exceptions require explicit, documented approval from the user's manager, the relevant data/system owner, and IT Cybersecurity, and will be subject to time-bound reviews to ensure continued necessity. *Rationale:* Adhering to role-based inheritance maintains the integrity and manageability of the RBAC system. Exceptions complicate auditing and can lead to "privilege creep."

**Table 1.3.A: User Roles and Default Access Privileges Matrix (Illustrative Extract)**

Role Name	Brief Role Description	Key Systems Accessed	Default Access Level (Illustrative)	Justification/PoLP Alignment
Bank Teller	Handles customer transactions at the branch.	Core Banking System (CBS) - Teller Module, Cash Mgmt System	CBS: Transact, Inquire. Cash Mgmt: Limited to own till.	Necessary for daily transaction processing, limited to specific functions to prevent fraud.
Loan Officer	Processes and manages loan applications.	Loan Origination System (LOS), CRM, CBS (Inquiry)	LOS: Create, Modify, Submit Apps. CRM: Read/Write Customer Data.	Required for loan processing lifecycle. Access to CBS for verification, not transaction.
Branch Manager	Oversees branch operations and staff.	CBS (Supervisor Module), CRM, HR Portal, Reporting Tools	CBS: Override, Approve limits. CRM: Team View. HR: Staff Mgmt.	Necessary for operational oversight, approvals, and staff management within the branch.
IT Support Analyst	Provides technical support to end-users.	ITSM System, Active Directory (User Mgmt), Endpoint Mgmt	AD: Reset Passwords, Unlock Accounts. Endpoint: Remote Assist.	Required for resolving user IT issues, limited to specific administrative tasks.
Database Administrator	Manages and maintains bank databases.	Database Servers, DB Mgmt Tools, Backup Systems	Full control over specific DB instances, restricted OS access.	Essential for database health, performance, and security. Access segmented by DB environment.

Compliance Auditor	Conducts internal audits for regulatory compliance.	Audit Mgmt Software, Read-Only access to various systems	Read-only to transaction logs, system configurations, IAM logs.	Required for audit functions, read-only to prevent data alteration and maintain independence.
--------------------	---	--	---	---

*This matrix serves as a clear, centralized reference for standard access provisioning, forms a practical tool for implementing RBAC and PoLP, supports audit activities by providing an authoritative source for comparison, aids in training, improves efficiency in provisioning, and demonstrates a structured approach to access management.*

## 1.4. Principle of Least Privilege (PoLP) Implementation

**1.4.1. PoLP Enforcement:** World Bank mandates the enforcement of the Principle of Least Privilege (PoLP) for all user accounts, system accounts, applications, and processes. This means that any entity (human or non-human) will be granted only the minimum necessary access rights, permissions, and system privileges required to perform its officially assigned duties or functions. *Rationale:* PoLP is a cornerstone of a robust security posture. It significantly reduces the potential attack surface, limits the propagation of malware should a system be compromised, and minimizes the potential damage that can be caused by accidental misuse or a malicious insider. NIST SP 800-53 control AC-6 specifically mandates the implementation of PoLP.

**1.4.2. Default Deny:** The default security posture for access to all World Bank resources (systems, applications, data, network segments) is "deny all." Access will only be explicitly granted when a legitimate business need has been identified, formally requested, and approved through the established access request process. *Rationale:* A "default deny" stance ensures that access is never granted implicitly or accidentally, forcing a conscious decision and justification for every access privilege.

**1.4.3. Granular Permissions:** Whenever technically feasible, permissions will be applied at the most granular level possible. This includes differentiating between read-only, write, delete, execute, and administrative permissions for specific data objects, system functions, or application modules. *Rationale:* Granular control allows for fine-tuning of access rights to precisely match job requirements, avoiding the over-provisioning of broad privileges.

**1.4.4. Application of PoLP to System Accounts:** The Principle of Least Privilege extends to all non-human identities, including service accounts used by applications, system accounts for operating system processes, and accounts used for automated tasks or inter-system communication. These accounts must be configured with only the permissions essential for their specific function and should not possess interactive login rights unless explicitly required and approved. *Rationale:* Compromise of a highly privileged service or system account can be particularly damaging. Restricting their permissions limits this risk.

The successful implementation of both RBAC and PoLP is not a one-time configuration task but an ongoing process. It is critically dependent on accurate and timely user provisioning during onboarding (ensuring new hires get only the access defined for their role), meticulous

de-provisioning during offboarding (ensuring all access is revoked promptly), and diligent periodic access reviews. Without these supporting procedures, roles can become misaligned with actual needs over time, and individuals may accumulate unnecessary privileges ("privilege creep"), thereby negating the security benefits that RBAC and PoLP are designed to provide. For example, if an employee transitions to a new role within the Bank but their access rights from the previous role are not revoked, their accumulated privileges could violate PoLP, even if the permissions for their new role are correctly defined and minimal. Similarly, if periodic access reviews are not conducted thoroughly, such discrepancies may persist undetected, increasing the risk exposure for the Bank.

## **1.5. Access Request and Approval Processes**

**1.5.1. Formal Access Request:** All requests for new access to systems, applications, or data, or for modifications to existing access levels, must be initiated through World Bank's designated IT Service Management (ITSM) platform. A standardized electronic access request form must be completed, providing details such as the user requiring access, the specific resources requested, the level of access needed, and a clear business justification for the request. *Rationale:* A formal, centralized process ensures consistency, trackability, and auditability of all access requests.

**1.5.2. Managerial Approval:** Every access request must first be reviewed and approved by the requesting user's direct line manager. The manager is responsible for validating the legitimacy of the business need for the requested access in relation to the user's current job role and responsibilities. *Rationale:* Managers are best positioned to understand their team members' roles and the access they genuinely require to perform their duties.

**1.5.3. Data/System Owner Approval:** For access to systems or data classified as sensitive, confidential, or restricted, or for access requests that deviate from standard role profiles, additional approval from the designated Data Owner or System Owner is mandatory. The Data/System Owner is accountable for the security and appropriate use of the resources under their stewardship. *Rationale:* Data/System Owners have a vested interest and responsibility in protecting their assets and ensuring access is granted appropriately. *Example:* A request for direct query access to the customer transaction database (classified as Restricted) by a data analyst would require approval from their manager and additionally from the Head of Retail Banking Operations, who is the designated System Owner for the Core Banking System.

**1.5.4. IT Security Review:** The IT Cybersecurity team reserves the right to review, and may be required to approve, access requests that involve high levels of privilege (e.g., administrative access), access to critical infrastructure components, or requests that represent a significant deviation from established role-based access profiles. This review will assess the potential security implications of granting the requested access. *Rationale:* Provides an additional layer of scrutiny for high-risk access requests, ensuring security best practices are considered.

**1.5.5. Audit Trail:** All stages of the access request and approval process, including the initial request, justifications, all approvals (managerial, data/system owner, IT Security), any denials, and the final provisioning actions, must be automatically logged within the ITSM system. This creates an auditable trail for compliance and review purposes. *Rationale:* A complete audit trail is essential for demonstrating due diligence, supporting investigations, and meeting regulatory requirements for access control.

## **1.6. Periodic Access Reviews and Recertification**

**1.6.1. Regular Review Schedule:** To ensure that access rights remain appropriate and comply with the Principle of Least Privilege, periodic access reviews and recertification are mandatory. \* **Standard User Access:** Line managers must review the access rights of their direct reports at least on a quarterly basis. \* **Privileged User Access:** Access rights for all privileged accounts (including system administrators, database administrators, and users with access to sensitive system configurations) must be reviewed more frequently, at least on a monthly basis, by their respective managers and the relevant system owners. *Rationale:* Regular reviews are crucial to identify and remove unnecessary access privileges that may have accumulated over time due to role changes, project completions, or oversight ("privilege creep"). This proactive process helps maintain a state of least privilege.

**1.6.2. Recertification Process:** During the review, managers and data/system owners must formally attest to the continued necessity of each access permission held by the users under their purview. They must either recertify the existing access as appropriate for the user's current job responsibilities or submit a request for modification (e.g., downgrade permissions) or complete revocation of access if it is no longer required. *Rationale:* Recertification forces an active decision on whether existing access is still justified, rather than allowing permissions to persist indefinitely.

**1.6.3. Automated Review Triggers:** In addition to scheduled periodic reviews, access reviews will be automatically triggered by specific events within the HR system or IAM system. These events include, but are not limited to: \* Employee transfer to a different department or role. \* Employee promotion. \* Employee returning from extended leave (e.g., sabbatical, long-term disability). \* Significant changes to a system or application that impact existing user permissions. *Rationale:* Event-driven reviews ensure that access rights are reassessed promptly when a user's circumstances change, rather than waiting for the next scheduled review.

**1.6.4. Documentation of Reviews:** All access review activities, including the list of users and permissions reviewed, the decisions made by reviewers (recertify, modify, revoke), justifications for these decisions, and any subsequent actions taken, must be thoroughly documented and retained as per the Bank's data retention policy. These records are critical for audit and compliance purposes. *Rationale:* Documentation provides evidence of due diligence in managing access rights and is essential for demonstrating compliance with regulatory requirements.

**1.6.5. Tools for Access Governance:** World Bank will leverage specialized access governance tools to the extent possible. These tools can help automate the access review and recertification process by generating reports of current access, routing review tasks to the appropriate personnel, tracking completion status, and providing dashboards for oversight. *Rationale:* Automation streamlines the review process, reduces manual effort, improves accuracy, and provides better visibility into the status of access certifications across the organization.

## **1.7. Emergency Access Procedures ("Break-Glass")**

**1.7.1. Defined Emergency Scenarios:** World Bank recognizes that exceptional circumstances may arise requiring immediate, temporary access to critical systems when standard access procedures cannot be followed or authorized personnel are unavailable. "Break-glass" procedures are established for such pre-defined and documented emergency scenarios. Examples include: \* A critical system outage impacting core banking operations outside of business hours, where the primary on-call administrator is unreachable. \* A security incident requiring immediate containment actions on a system by personnel who do not normally have such privileges. \* A natural disaster rendering primary administrative staff inaccessible. *Rationale:* Having a formal emergency access procedure ensures that critical issues can be addressed promptly while maintaining a degree of control and accountability, even in crisis situations.

**1.7.2. Approval for Emergency Access:** Granting emergency access is a high-risk activity and requires stringent approval. Such access must be authorized by at least two designated senior managers. Approved authorizers may include the on-duty Chief Information Officer (CIO) or delegate, the Head of Security Operations, or an equivalent level of management as defined in the emergency contact roster. Approval must be documented, even if initially verbal, followed by formal written confirmation. *Rationale:* Requiring multiple senior-level approvals provides a check and balance for granting extraordinary access, reducing the risk of misuse.

**1.7.3. Temporary and Monitored Access:** Emergency access will always be: \* **Temporary:** Granted for the minimum duration necessary to resolve the emergency. \* **Specific:** Limited to the specific systems and actions required to address the crisis. \* **Unique Credentials:** Provided using unique, one-time, or strictly time-limited credentials that are distinct from any user's standard account. Generic or shared emergency accounts are prohibited. \* **Monitored:** All actions performed using emergency access credentials will be logged with the highest level of detail and subject to real-time monitoring by the Security Operations Center (SOC) where feasible. *Rationale:* These measures limit the window of opportunity for misuse and ensure that all activities performed under emergency access are traceable and scrutinized.

**1.7.4. Post-Emergency Review:** Every instance of emergency access usage must be formally reviewed by the IT Cybersecurity team and the relevant system owner(s) within 24 hours of the access being revoked. This review will verify the legitimacy of the access, the appropriateness



of actions taken, and ensure that access was terminated promptly after the emergency was resolved. A report detailing the incident, the access granted, actions performed, and review findings must be documented and retained. *Rationale:* Post-emergency review ensures accountability, identifies any potential misuse, and provides an opportunity to refine emergency procedures.

### **1.8. Password Management Guidelines (Summary)**

A comprehensive Password Policy is maintained by World Bank and must be adhered to by all users. Key tenets relevant to identity management include:

**1.8.1. Password Change Frequency:** Users are required to change their passwords at regular, system-enforced intervals. For standard user accounts, this interval is typically every 90 days. For privileged accounts, a more frequent change interval, such as every 60 days, is enforced. *Rationale:* Regular password changes limit the time window during which a compromised password can be exploited.

**1.8.2. Prohibition of Password Sharing:** Sharing of passwords with any other individual, including colleagues, managers, IT support staff, or family members, is strictly prohibited. Each user is solely responsible for the confidentiality of their own password. *Rationale:* Password sharing undermines individual accountability and significantly increases security risks.

**1.8.3. Secure Password Storage:** Users must not write down passwords in easily accessible locations (e.g., sticky notes on monitors, under keyboards) or store them in unsecured electronic files or applications. World Bank encourages and may provide approved password manager tools to help users create and securely store complex, unique passwords for their various accounts. *Rationale:* Insecurely stored passwords can be easily discovered and misused.

**1.8.4. Password History:** Bank systems will enforce a password history mechanism, preventing users from reusing a specified number of their most recent passwords (e.g., the last 12 passwords). This helps to ensure that if an old password is compromised, it cannot be simply reused. *Rationale:* Prevents attackers from using previously compromised passwords if users attempt to revert to them.

The strength of these technical password controls is directly linked to user behavior and awareness. Even the most stringent password complexity and change frequency rules can be undermined if users adopt insecure practices like writing passwords down or falling victim to phishing attacks that harvest credentials. Therefore, these IAM procedures must be complemented by robust and continuous security awareness training, as detailed in the Security Code of Conduct and Onboarding/Offboarding Procedures. This training must emphasize the personal responsibility each user has in protecting their credentials and recognizing threats. Clear communication channels for reporting lost or suspected compromised credentials are also vital to quickly mitigate potential damage.

## 1.9. Session Management

**1.9.1. Session Timeouts:** To mitigate the risk of unauthorized access to unattended active sessions, all interactive sessions on World Bank workstations and critical applications will automatically time out after a predefined period of inactivity. A typical timeout period is 15 minutes. Upon timeout, the user will be required to re-authenticate to resume their session. *Rationale:* Prevents unauthorized individuals from using a workstation or application if it's left logged in and unattended.

**1.9.2. Screen Locking:** Users are required to manually lock their workstation screens (e.g., by pressing Windows Key + L or Ctrl+Alt+Del then Lock) whenever they step away from their desk, even for short periods. Additionally, automatic screen locking will be enforced system-wide after a shorter period of inactivity, typically 5 minutes. *Rationale:* A primary defense against opportunistic unauthorized access to an unattended workstation.

**1.9.3. Concurrent Session Limits:** For certain critical applications or user roles, World Bank may impose limits on the number of concurrent active sessions allowed for a single User ID. This helps to prevent account sharing and can indicate anomalous activity if limits are unexpectedly reached. *Rationale:* Can help detect account sharing or unauthorized use of credentials across multiple locations or devices simultaneously.

## 1.10. Remote Access Security for Identities

**1.10.1. VPN Requirement:** All remote access from outside World Bank's trusted network to the Bank's internal network, systems, or applications must be established exclusively through the Bank-approved Virtual Private Network (VPN) solution. Direct connections to internal resources from the internet are prohibited. *Rationale:* VPNs create an encrypted tunnel, protecting data in transit and providing a controlled entry point into the corporate network.

**1.10.2. MFA for VPN:** Multi-Factor Authentication (MFA) is a mandatory requirement for all VPN authentication attempts. Users must provide their standard credentials plus a second factor (e.g., code from an authenticator app, hardware token) to establish a VPN connection. *Rationale:* Significantly strengthens the security of remote access, protecting against compromised passwords.

**1.10.3. Endpoint Security for Remote Devices:** Any device, whether Bank-owned or personally owned (if permitted under a BYOD policy), used to access World Bank resources remotely must meet the Bank's minimum endpoint security standards. These standards typically include having an up-to-date operating system with all security patches applied, active and updated antivirus/anti-malware software, and full-disk encryption enabled. Non-compliant devices may be blocked from accessing the VPN. *Rationale:* Ensures that the device connecting to the Bank's network is not already compromised, which could then introduce threats into the internal environment.

**1.10.4. Split Tunneling Prohibition:** Split tunneling on VPN connections is strictly prohibited. When a user is connected to the World Bank VPN, all internet traffic from their remote device

must be routed through the Bank's network and security controls (e.g., web filters, intrusion detection systems). This prevents the remote device from simultaneously accessing the internet directly, which could create a bypass for security measures or an attack vector.

*Rationale:* Ensures all traffic from remote endpoints is subject to the Bank's security monitoring and filtering, preventing exposure to threats from the open internet while connected to internal resources.

### **1.11. Third-Party Access Management**

**1.11.1. Vendor Risk Assessment:** Before any third-party vendor, contractor, or consultant is granted access to World Bank systems or data, they must undergo a formal security risk assessment conducted by the IT Cybersecurity and Vendor Management teams. The level of scrutiny will be commensurate with the sensitivity of the data or systems they will access and the nature of the services they provide. *Rationale:* Ensures that third parties meet the Bank's security standards before being allowed access to its environment, mitigating supply chain risks.

**1.11.2. Dedicated Third-Party Accounts:** Third-party users will always be provisioned with unique, named User IDs. The use of shared, generic, or anonymous accounts for third-party access is strictly prohibited. Each third-party individual requiring access must have their own distinct account. *Rationale:* Ensures accountability and traceability for actions performed by third-party personnel.

**1.11.3. Time-Bound Access:** Access for third-party users will be granted for a strictly limited and predefined duration, directly aligned with the terms of their contract or engagement with World Bank. All third-party access rights must be reviewed regularly (e.g., quarterly or upon contract milestones) and automatically expire or be revoked upon contract termination or completion of the engagement. *Rationale:* Prevents indefinite access for third parties and ensures access is removed promptly when no longer needed.

**1.11.4. PoLP for Third Parties:** The Principle of Least Privilege will be rigorously applied to all third-party access. Vendors and contractors will only be granted the minimum necessary permissions to perform their specific, contracted duties. Access to systems or data outside the direct scope of their engagement is forbidden. *Rationale:* Limits the potential impact if a third-party account is compromised or misused.

**1.11.5. Monitoring of Third-Party Access:** All access attempts and activities performed by third-party users within World Bank systems will be logged and actively monitored by the Security Operations Center (SOC). Any anomalous or suspicious activity will trigger an alert and investigation. *Rationale:* Provides oversight of third-party actions and allows for rapid detection of potential security incidents originating from external partners.

### **1.12. Monitoring and Auditing of Identity Activities**

**1.12.1. Logging of IAM Events:** All significant IAM-related events across World Bank systems must be comprehensively logged. This includes, but is not limited to: \* Successful and failed

login attempts. \* Password change and reset events. \* MFA challenge successes and failures. \* Account lockouts and unlocks. \* Creation, modification, and deletion of user accounts. \* Granting, modification, and revocation of access privileges. \* Use of privileged accounts. \* Emergency access events. Detailed requirements for logging are specified in the "Logging and Monitoring Policy" (Document 6). *Rationale:* Comprehensive logging is essential for security monitoring, incident response, forensic analysis, and compliance reporting.

**1.12.2. Regular Audit Log Reviews:** The IT Cybersecurity team and/or the Security Operations Center (SOC) will conduct regular, systematic reviews of IAM audit logs. These reviews aim to detect anomalies, patterns of unauthorized access attempts, policy violations, or other suspicious activities that may not trigger automated alerts. *Rationale:* Proactive log review can uncover subtle or emerging threats that automated systems might miss.

**1.12.3. Alerts for Suspicious Activity:** Automated alerts will be configured within the Security Information and Event Management (SIEM) system and other monitoring tools to provide real-time notification of potentially malicious or anomalous IAM activities. Examples include: \* Multiple failed login attempts for a single account or from a single IP address. \* Login attempts from geographically improbable locations. \* Attempts to use disabled or terminated accounts. \* Unauthorized privilege escalation attempts. \* Access to sensitive systems outside of normal business hours (if applicable to the role). *Rationale:* Real-time alerts enable rapid detection and response to potential security incidents, minimizing their impact.

Effective IAM is a cornerstone for meeting broader regulatory obligations. Deficiencies in identifying users, controlling their access, or monitoring their activities can lead to significant compliance failures under regulations like FFIEC , GLBA , and the Sarbanes-Oxley Act (SOX). For example, FFIEC guidance explicitly details requirements for robust authentication methods, comprehensive access management programs including regular user access reviews, and the implementation of MFA, especially for high-risk users and systems. GLBA's mandate to protect customer financial information inherently relies on strong IAM controls to prevent unauthorized access. SOX requires stringent controls over financial reporting systems, and IAM is key to ensuring that only authorized personnel can access, modify, or report on financial data. Therefore, the thoroughness of this IAM document and the diligence with which its procedures are followed directly impact World Bank's ability to demonstrate compliance and avoid potentially severe penalties and reputational damage.

## **1.13. User Responsibilities for Identity Protection**

**1.13.1. Credential Protection:** All users are personally responsible for the security and confidentiality of the credentials assigned to them by World Bank. This includes User IDs, passwords, PINs, responses to security questions, hardware tokens, software tokens, smartcards, and any biometric data used for authentication. Credentials must not be shared, displayed, or stored insecurely. *Rationale:* Emphasizes that identity security is a shared responsibility, and users play a critical role in protecting their own access.

**1.13.2. Reporting Suspicious Activity:** Users must immediately report any suspected compromise of their credentials, any unauthorized activity observed on their accounts, or any other suspicious security-related incidents to the IT Help Desk or directly to the Security Operations Center (SOC) through designated channels. Prompt reporting is crucial for timely investigation and mitigation. *Rationale:* Users are often the first to notice anomalies related to their accounts; empowering them to report helps in early threat detection.

**1.13.3. Compliance with IAM Policies:** All users are required to read, understand, and comply with all World Bank Identity and Access Management policies, procedures, and standards, including this document and the Security Code of Conduct. *Rationale:* Ensures that users are aware of their obligations and the rules governing access to Bank resources.

#### **1.14. Reporting Lost/Compromised Credentials**

**1.14.1. Immediate Reporting:** If a user loses any physical authentication token (e.g., smartcard, hardware token) or suspects that their password or other credentials have been compromised (e.g., due to a phishing attempt, malware infection, or inadvertent disclosure), they must report this immediately to the IT Help Desk. Delay in reporting can significantly increase the risk of unauthorized access. *Rationale:* Immediate reporting allows IT and Security teams to take swift action to disable compromised credentials and prevent misuse.

**1.14.2. Account Disablement/Password Reset:** Upon receiving a report of lost or compromised credentials, the IT Help Desk or Security team will take immediate action. This will typically involve temporarily disabling the affected user account, resetting the password, and/or deactivating the compromised token. The user will be guided through the process of re-establishing secure access. *Rationale:* Contains the potential damage by preventing further use of the compromised credentials.

**1.14.3. Incident Investigation:** All reported incidents of lost or compromised credentials will be logged and investigated by the IT Cybersecurity team. The investigation will aim to determine the cause and scope of the compromise, identify any unauthorized access or data exposure that may have occurred, and recommend corrective actions to prevent recurrence. *Rationale:* Helps understand the threat vector and improve security controls based on lessons learned.

#### **1.15. Consequences of Non-Compliance**

Failure to comply with these Identity Management Rules and Procedures, or any other World Bank security policy, may result in disciplinary action. Such actions will be determined based on the severity and nature of the violation and will be administered in accordance with World Bank's established disciplinary policy and applicable local labor laws. Consequences can range from verbal or written warnings to suspension, and up to and including termination of employment or contract. Furthermore, certain violations, particularly those involving intentional misuse of access or compromise of sensitive data, may lead to legal action, including civil liability or criminal prosecution. *Rationale:* Clearly outlines the seriousness of

adhering to IAM policies and the potential repercussions for violations, reinforcing the importance of security. The potential for hefty fines, loss of customer trust, and operational delays resulting from security breaches or regulatory non-compliance underscores the critical nature of these rules.

#### **1.16. Policy Review and Updates**

These Identity Management Rules and Procedures will be reviewed at least annually by the IT Cybersecurity department, in consultation with HR, IT Operations, and relevant business units. Updates will be made as necessary to reflect changes in World Bank's technology environment, evolving business requirements, the regulatory landscape, emerging cybersecurity threats, and industry best practices. Approved changes will be communicated to all affected personnel. *Rationale:* Ensures the IAM framework remains current, effective, and aligned with the Bank's evolving needs and risk environment.