

# Procedures for Onboarding/Offboarding

## 3.1. Introduction

**Purpose:** This document outlines the standardized, secure, and efficient procedures for the onboarding of new personnel into World Bank and the offboarding of departing personnel. The primary objectives are to ensure that appropriate access to Bank systems and resources is granted in a timely and controlled manner for new hires, and that all access is promptly and completely revoked for departing individuals, thereby minimizing security risks and ensuring operational continuity.

**Scope:** These procedures apply to all individuals involved in the personnel lifecycle processes at World Bank. This includes, but is not limited to, hiring managers, Human Resources (HR) personnel, Information Technology (IT) staff (including helpdesk, system administrators, and network teams), Cybersecurity team members, Physical Security staff, and the departing employees themselves. The procedures cover full-time and part-time employees, contractors, consultants, and temporary staff.

**Responsibilities:** The successful execution of these procedures relies on clear delineation and diligent performance of responsibilities by various departments:

- \* **Human Resources (HR):** Initiates onboarding upon offer acceptance and offboarding upon notification of departure. Manages all employment-related paperwork, conducts background checks (or coordinates them), facilitates orientation, conducts exit interviews, and ensures legal and regulatory compliance related to employment.
- \* **Hiring Manager/Supervisor:** Defines access requirements for new hires based on their role, submits access requests, ensures knowledge transfer during offboarding, and confirms return of physical assets from departing team members.
- \* **Information Technology (IT) Department:** Provisions and de-provisions user accounts and access to systems and applications. Manages the issuance, tracking, and recovery of IT assets (laptops, mobile devices, tokens). Provides technical support during onboarding.
- \* **Cybersecurity Team:** Defines security policies related to access, oversees compliance with these procedures, may conduct risk assessments for certain roles, and investigates any security anomalies during these processes. Enforces access policy adherence.
- \* **Physical Security Department:** Manages the issuance and revocation of physical access badges and keys.

**Rationale:** Clear responsibilities are crucial for a smooth and secure process, ensuring no critical steps are missed. The collaborative nature of these processes, involving HR, IT, Finance, and Managers, is essential for comprehensive coverage.

## 3.2. Onboarding Procedures

The onboarding process is a critical control point for integrating new personnel into World Bank's security culture and ensuring they receive appropriate access from day one. This process sets the foundation for their understanding of security responsibilities.

**3.2.1. Pre-Employment Screening & Verification:** \* Prior to the first day of employment, HR, or a designated third-party agency, will conduct thorough background checks. The extent of these checks will be appropriate for the role and the level of access to sensitive financial data or critical systems the individual will have. Checks may include identity verification, criminal record checks (especially for offenses involving breach of trust or financial misconduct as per FDIA requirements), employment history verification, and education verification. For certain roles, credit history checks may also be performed in compliance with applicable laws. \* All identity documents provided by the new hire must be verified for authenticity. *Rationale:* Background checks are vital in the financial industry to mitigate risks associated with hiring individuals who may pose a threat to the Bank's assets or reputation.

**3.2.2. HR Onboarding Initiation:** \* Upon formal acceptance of an employment offer, HR initiates the onboarding workflow within the Bank's Human Resource Information System (HRIS). \* HR is responsible for collecting all necessary personal information for payroll, benefits enrollment, and emergency contact details (e.g., direct deposit forms, tax withholding forms). *Rationale:* Establishes the official record for the new employee and triggers downstream processes.

**3.2.3. IT Account and Access Provisioning Request:** \* The hiring manager is responsible for submitting a formal IT access request for the new hire via the Bank's IT Service Management (ITSM) system. This request must be submitted with sufficient lead time before the start date. \* The request must specify the new hire's role, department, start date, and the required IT accounts (e.g., network login, email, core banking application access, CRM access). Access requirements should be based on predefined role profiles documented in the Bank's RBAC matrix (refer to Document 1: Identity Management). *Rationale:* Ensures that access is requested based on legitimate business need and role requirements.

**3.2.4. Account Creation and Credential Issuance:** \* Based on the approved access request, the IT department provisions all necessary accounts with unique User IDs. \* Initial passwords for new accounts are generated securely and provided to the new hire through a secure mechanism (e.g., a temporary password delivered separately, requiring an immediate change upon first login). \* Instructions for enrolling in and using the Bank's Multi-Factor Authentication (MFA) system are provided, and MFA is configured for the user's accounts as per policy. *Rationale:* Establishes the digital identity for the new hire and provides initial secure access.

**3.2.5. Access Rights Assignment:** \* Access permissions are assigned strictly in accordance with the approved role profile and the Principle of Least Privilege (PoLP). Only the minimum necessary access to perform the job duties will be granted. \* Any request for access permissions that deviate from or exceed the standard profile for the assigned role requires additional documented justification from the hiring manager and specific approval from the relevant data/system owner and potentially the IT Cybersecurity team. *Rationale:* Enforces PoLP from the outset, minimizing the risk of excessive privileges.

**3.2.6. Issuance of Company Assets:** \* The IT department issues and records all company-owned IT assets provided to the new hire, such as laptops, mobile phones, security tokens, software licenses, and physical access badges. \* The new hire must formally acknowledge receipt of these assets, typically by signing an asset issuance form. This form details the assets provided and the user's responsibility for their care and return. *Rationale:* Ensures accountability for Bank property and tracks asset allocation.

**3.2.7. Security Awareness Training Enrollment & Policy Acknowledgement:** \* The new hire is automatically enrolled in World Bank's mandatory initial security awareness training program. This training must be completed within a specified timeframe (e.g., the first week of employment). Embedding security awareness training into the onboarding process is crucial for enhancing the organization's cyber resilience, as new hires may be unfamiliar with company protocols and particularly vulnerable. Training should commence from day one to instill a security-first mindset. \* The new hire must review and formally acknowledge their understanding and acceptance of key Bank policies, including the Security Code of Conduct (Document 2), Acceptable Use Policy, Data Privacy Policy, and this Onboarding/Offboarding Procedure. These acknowledgements are tracked by HR. *Rationale:* Ensures new hires are immediately aware of their security responsibilities and the Bank's expectations.

**3.2.8. Physical Access Setup:** \* The Physical Security department, based on information from HR and the hiring manager, provisions appropriate physical access rights for the new hire. This includes access to Bank buildings, specific floors, or departments, programmed into their employee access badge. *Rationale:* Controls physical entry to Bank premises based on role and location.

**3.2.9. Secure Workstation Setup Guidance:** \* The new hire receives guidance from IT or their manager on securely setting up their physical and virtual workstation. This includes advice on password management for their initial login, screen locking practices, proper handling of any physical documents, and securing their immediate work area. *Rationale:* Promotes secure work habits from the beginning.

**3.2.10. Introduction to Reporting Security Incidents:** \* During orientation or initial IT setup, the new hire is informed about the procedures for reporting any suspected security incidents, vulnerabilities, or concerns. Contact information for the IT Help Desk and the Security Operations Center (SOC) is provided. *Rationale:* Ensures new hires know how to report potential security issues promptly.

**3.2.11. Mentor Assignment (Recommended):** \* Where appropriate, the hiring manager may assign an experienced team member as a mentor to the new employee. The mentor can provide guidance on day-to-day tasks, company culture, and reinforce understanding of security practices and policies in a practical context. *Rationale:* Facilitates smoother integration and provides an informal channel for security reinforcement.

**3.2.12. Initial Review Meeting:** \* The hiring manager should schedule a check-in meeting with the new hire within their first week of employment. This meeting is an opportunity to

discuss initial progress, answer questions, and specifically address any security-related queries or concerns the new hire might have. *Rationale:* Provides early support and clarifies expectations, including those related to security.

**3.2.13. Documentation of Onboarding Completion:** \* All key steps in the onboarding process, particularly those related to security access, asset issuance, training completion, and policy acknowledgements, are tracked and documented using a standardized onboarding checklist. This checklist is maintained by HR and/or the hiring manager. *Rationale:* Provides an auditable record that all required onboarding procedures were completed.

**3.2.14. System Access Verification:** \* Within the first few days, the new hire and their manager should verify that all provisioned system access is correct, functional, and aligns with the requirements of the role. Any discrepancies must be reported immediately to the IT Help Desk. *Rationale:* Confirms that the provisioning process was successful and the user has the necessary tools.

**3.2.15. Compliance Training (Role-Specific):** \* Based on their specific role within the financial services environment, the new hire will be enrolled in mandatory compliance training relevant to their responsibilities. This may include training on Anti-Money Laundering (AML), Know Your Customer (KYC) procedures, Sarbanes-Oxley (SOX) compliance, or other regulatory requirements. *Rationale:* Ensures employees in the financial sector are aware of and comply with critical industry-specific regulations.

**Table 3.A: Onboarding IT Security Checklist**

Task Item	Responsible Party	Date Completed	Verified By (Signature/Timestamp)	Notes/Exceptions
Background Check Completed & Cleared	HR			Level of check appropriate for role.
Identity Verified	HR			
IT Access Request Submitted by Manager	Hiring Manager			Based on RBAC Profile.
Unique User ID Created	IT			
Network Account Provisioned	IT			
Email Account Provisioned	IT			
Core Application Accounts Provisioned (as per role)	IT			e.g., CBS, LOS, CRM.
Initial Credentials Securely Issued	IT			Password change on first login enforced.
MFA Enrolled & Tested	New Hire / IT			
Role-Based Access Permissions Assigned per Matrix	IT			Verified against approved role.

Laptop/Desktop Issued & Recorded	IT			Serial number, model recorded.
Mobile Device Issued & Recorded (if applicable)	IT			IMEI, serial number recorded.
Security Token(s) Issued & Recorded (if applicable)	IT			Token serial number recorded.
Physical Access Badge Issued & Programmed	Physical Security / HR			
Security Awareness Training Scheduled/Completed	New Hire / HR			Within first week.
Security Code of Conduct Acknowledged (Signed)	New Hire / HR			
Acceptable Use Policy Acknowledged (Signed)	New Hire / HR			
Data Privacy Policy Acknowledged (Signed)	New Hire / HR			
Incident Reporting Procedure Briefing Provided	Hiring Manager / IT			
System Access Functionality Verified	New Hire / Hiring Manager			Report discrepancies to IT Help Desk.
Role-Specific Compliance Training Enrolled	HR / Hiring Manager			e.g., AML, KYC.

### Esporta in Fogli

*This checklist ensures consistency and completeness in executing critical security steps for every new hire, assigns clear accountability, provides an essential audit trail for compliance, streamlines the onboarding workflow, and ultimately reduces risk by ensuring new personnel start with correct access and foundational security knowledge.*

### 3.3. Offboarding Procedures

Effective and timely offboarding is a critical security function. Failure to promptly revoke access and recover assets from departing personnel can create significant vulnerabilities, including the risk of data breaches by disgruntled former employees or the exploitation of dormant accounts. Studies indicate a high percentage of former employees retain access to company applications post-departure, making offboarding a major security concern for IT leaders.

**3.3.1. Notification of Departure:** \* The departing employee must provide their formal resignation to their direct manager and to the Human Resources department. \* Upon receipt of resignation or decision of termination, HR immediately initiates the offboarding process in the HRIS and formally notifies the IT department, IT Cybersecurity team, Physical Security department, the employee's manager, and any other relevant departments (e.g., Finance for

final payroll) of the employee's departure and their official last working day. This notification must be timely to allow for proper planning of access revocation. *Rationale:* Triggers all necessary offboarding workflows across departments.

**3.3.2. Access Revocation Plan:** \* Upon notification of departure, the IT department and IT Cybersecurity team will immediately formulate a plan for the systematic revocation of all logical (system, application, network, remote) and physical access rights. \* This plan will ensure that all access is scheduled to be terminated precisely at the end of the employee's last working day, or immediately in the case of involuntary termination for cause. The prompt removal of access is paramount to prevent any unauthorized activity by former employees. *Rationale:* Proactive planning ensures access is cut off at the exact, appropriate time.

**3.3.3. Knowledge Transfer and Data Handover:** \* The hiring manager is responsible for ensuring that the departing employee completes all necessary knowledge transfer activities. This includes documenting critical processes, ongoing projects, key contacts, and any specialized knowledge relevant to their role. \* All World Bank-related data, files, documents, and intellectual property created or managed by the departing employee must be securely transferred to a designated current employee or to secure Bank-controlled storage. The departing employee must not retain any copies of Bank data on personal devices or accounts. *Rationale:* Ensures business continuity and protects Bank intellectual property.

**3.3.4. Return of Company Assets:** \* On or before their last working day, the departing employee must return all World Bank company assets to their manager or the IT department. This includes, but is not limited to, laptops, mobile phones, tablets, security tokens, access badges, keys, corporate credit cards, physical files, and any other Bank property. \* A formal "Employee Asset Return Form" must be completed, listing all returned items. This form should be signed by the departing employee and their manager (or an IT representative) to confirm the return of all assets. Failure to return assets can have financial and legal implications. *Rationale:* Recovers valuable Bank property and prevents potential misuse or data loss from unreturned devices.

**3.3.5. Revocation of Logical Access:** \* Precisely at the scheduled time of departure (or immediately upon termination), the IT department will disable or delete all the departing employee's logical access credentials. This includes: \* Network login accounts (e.g., Active Directory). \* Email accounts. \* Access to all business applications (core banking, CRM, ERP, etc.). \* Database access. \* Access to cloud services and SaaS applications used by the Bank. \* VPN and other remote access capabilities. *Rationale:* This is a critical step to prevent any post-employment access to Bank systems and data.

**3.3.6. Revocation of Physical Access:** \* The departing employee's physical access badge and any physical keys to Bank premises or secure areas must be collected by their manager or Physical Security on their last day. \* Physical access rights associated with their badge must be immediately deactivated in the physical access control system. *Rationale:* Prevents unauthorized physical entry after employment ends.

**3.3.7. Exit Interview:** \* HR will conduct an exit interview with the departing employee. This interview may cover reasons for departure, feedback on their employment experience, and will also serve as an opportunity to remind the employee of their ongoing confidentiality obligations and to confirm the return of all company assets and data. *Rationale:* Gathers feedback for organizational improvement and reinforces post-employment obligations.

**3.3.8. Final Payroll and Benefits Processing:** \* The Finance and HR departments will coordinate to process the employee's final paycheck, including any accrued vacation pay or other entitlements, in accordance with Bank policy and applicable labor laws. \* HR will provide the departing employee with information regarding the continuation of benefits (e.g., COBRA in the U.S.), status of retirement plans, and other relevant post-employment details. *Rationale:* Ensures all financial and benefits-related matters are concluded correctly.

**3.3.9. Account Archival/Deletion:** \* User accounts are disabled immediately upon departure. Depending on World Bank's data retention policies and any applicable legal holds, the user's data (e.g., email mailbox, network home drive) may be archived for a specified period before being securely and permanently deleted. \* If operationally necessary and approved by management and IT Security, email forwarding to a manager or designated colleague may be set up for a limited, defined period. *Rationale:* Balances the need to remove access with requirements for data retention and potential business continuity for a short period.

**3.3.10. Legal/Compliance Holds:** \* If the departing employee or their data is subject to any ongoing legal investigation, litigation hold, or specific regulatory compliance preservation order, their data, accounts, and associated logs will be preserved in accordance with instructions from the Legal and Compliance departments, overriding standard deletion schedules. *Rationale:* Ensures compliance with legal obligations to preserve evidence or records.

**3.3.11. Communication of Departure:** \* The manager is responsible for communicating the employee's departure to their team members and relevant internal and external stakeholders (e.g., clients, vendors, if appropriate). This communication should include information on how the departing employee's responsibilities will be covered and new points of contact. *Rationale:* Ensures smooth transition of work and maintains clear communication lines.

**3.3.12. Review of Shared/Service Account Credentials:** \* If the departing employee had knowledge of or access to any shared account credentials (e.g., departmental accounts, vendor portal logins used by a team) or administrative credentials for service accounts, these passwords must be changed immediately upon their departure. *Rationale:* Prevents potential misuse of shared credentials by a former employee.

**3.3.13. Documentation of Offboarding Completion:** \* All key steps in the offboarding process, especially those pertaining to security (access revocation, asset return), are meticulously tracked and documented using a standardized offboarding checklist. This checklist is completed and signed off by HR, the manager, and IT, and retained for audit

purposes. *Rationale:* Provides an auditable record that all required offboarding security measures were taken.

**3.3.14. Removal from Distribution Lists and Communication Groups:** \* The departing employee must be promptly removed from all internal email distribution lists, collaborative messaging platforms (e.g., Microsoft Teams, Slack), internal directories, and any other Bank communication groups. *Rationale:* Prevents continued receipt of internal communications and access to collaboration platforms.

**3.3.15. Third-Party Account Deactivation:** \* If the departing employee had accounts with third-party services or vendor portals that were used on behalf of World Bank (e.g., access to a cloud service provider console, industry association memberships paid by the Bank), HR or the manager must ensure these accounts are either deactivated, transferred to another employee, or that the Bank's association with the account is removed. *Rationale:* Closes potential backdoors through external services linked to the former employee.

The increasing trend towards automating onboarding and offboarding processes, as highlighted by solutions from identity management providers and specialized tools, is driven by a critical need within organizations like World Bank. This need stems from the demand for greater speed, unwavering consistency, and a significant reduction in human error, particularly in security-sensitive steps such as access provisioning and, more critically, access revocation. For World Bank, investing in new automation tools or optimizing existing ones for these personnel lifecycle events is not just an efficiency gain but a crucial enhancement to its security posture. Automation can directly link HR system events (e.g., new hire entry, termination processing) to IAM and ITSM system actions, ensuring that access rights are granted correctly based on roles from day one and, crucially, revoked comprehensively and immediately upon an employee's departure. This minimizes the window of vulnerability associated with manual delays or oversights, directly addressing a common and high-risk audit finding.

**Table 3.B: Offboarding IT Security Checklist**

Task Item	Responsible Party	Date/Time Completed	Verified By (Signature/Timestamp)	Notes/Exceptions
Departure Notified to IT/Cybersecurity/Physical Security by HR	HR			Include last working day/time.
Knowledge Transfer Plan Executed & Confirmed by Manager	Manager / Departing Employee			Documentation updated, projects handed over.
All Company Assets Inventoried & Returned (Asset Return Form Signed)	Departing Employee / Manager / IT			Laptop, mobile, tokens, badges, keys, documents, etc.
Network Login Account Disabled/Deleted	IT			Timestamp of action.



Email Account Disabled/Archived/Forwarded (as per policy)	IT			Forwarding only temporary & approved.
Access to All Business Applications Revoked	IT			CBS, CRM, LOS, financial systems, etc.
Access to Cloud Services & SaaS Applications Revoked	IT			
VPN and Remote Access Privileges Revoked	IT			
Database Access Privileges Revoked	IT / DBA			
Physical Access Badge Deactivated & Collected	Physical Security / Manager			
Physical Keys Collected (if applicable)	Manager			
Corporate Credit Card Returned & Cancelled (if applicable)	Manager / Finance			
Shared/Service Account Passwords Changed (if employee had access)	IT / System Owner			Document which passwords were changed.
Removed from All Internal Email Distribution Lists	IT / Manager			
Removed from Collaboration Platforms (Teams, Slack, etc.)	IT / Manager			
Removed from Internal Directories	IT / HR			
Third-Party/Vendor Accounts (used for Bank business) Deactivated	Manager / IT			
Legal/Compliance Hold Status Checked & Data Preserved (if applicable)	HR / Legal / IT			
Exit Interview Conducted (Security points covered)	HR			Confirmation of asset return, confidentiality reminder.

#### Esporta in Fogli

*This checklist is critical for ensuring the timely and complete revocation of all access and the recovery of all Bank assets, which are paramount security priorities during employee offboarding. It directly mitigates insider risks, provides auditable proof of due diligence for compliance purposes, ensures company property is recovered, and helps prevent the accumulation of orphaned accounts that could be exploited.*

### 3.4. Role Change/Internal Transfer Procedures

When an employee transitions to a new role or department within World Bank, the process must be managed with the same diligence as onboarding and offboarding to ensure access rights remain appropriate.

**3.4.1. Treat as Partial Offboarding/Onboarding:** An internal transfer or significant role change should be treated as a combination of offboarding from the old role and onboarding to the new role. This requires a formal review and adjustment of access privileges. *Rationale:* Prevents accumulation of unnecessary privileges from previous roles.

**3.4.2. Revoke Unnecessary Access:** The employee's manager for the old role, in coordination with IT, must ensure that all access rights, permissions, and system privileges that are not required for the new role are promptly revoked. This should occur on or before the effective date of the transfer. *Rationale:* Enforces PoLP by removing access that is no longer job-relevant.

**3.4.3. Grant New Access:** The employee's manager for the new role must submit a formal access request for any new systems or elevated permissions required for the new position. This request will follow the standard access request and approval process, adhering to RBAC profiles and PoLP. *Rationale:* Ensures new access is formally justified and approved.

**3.4.4. Manager Responsibility:** Both the outgoing manager and the incoming manager share responsibility for ensuring a smooth and secure transition of access rights. They must communicate effectively with each other, the employee, and the IT department to coordinate the revocation of old access and the provisioning of new access. *Rationale:* Ensures accountability and coordination during the transition.

### **3.5. Documentation and Record Keeping**

Meticulous record-keeping is essential for demonstrating compliance and for audit purposes.

**3.5.1. Maintenance of Checklists:** Completed and signed onboarding checklists (Table 3.A) and offboarding checklists (Table 3.B) for all personnel actions must be securely retained by the Human Resources department and/or the IT department, in accordance with the Bank's data retention policy. *Rationale:* Provides an auditable trail of procedural adherence.

**3.5.2. Asset Tracking Records:** The IT department must maintain accurate and up-to-date records of all Bank-owned IT assets issued to employees and the return of these assets upon departure or role change. This includes serial numbers, asset tags, dates of issuance and return, and user acknowledgements. *Rationale:* Essential for asset management, inventory control, and financial accountability.

**3.5.3. Access Request and Approval Logs:** All electronic access requests, manager approvals, data/system owner approvals, IT Security reviews, and provisioning/de-provisioning actions logged within the ITSM system must be retained as per the Bank's data retention and audit log policies. *Rationale:* Provides a detailed history of all access control decisions and actions.

The effectiveness of the entire Identity and Access Management lifecycle, as detailed in Document 1, fundamentally hinges on the meticulous execution of these onboarding and offboarding procedures. Correct initial provisioning based on RBAC and PoLP during onboarding ensures that users start with appropriate and minimal access. Conversely, timely and complete revocation of all access privileges during offboarding is crucial to prevent lingering access that could be exploited. Furthermore, information gathered during pre-employment screening, such as background checks, informs the initial risk assessment of a new identity and can influence the level of scrutiny or type of access granted. This highlights a strong interdependency: IAM rules are only as effective as their consistent application during these critical personnel lifecycle events.

### **3.6. Procedure Review and Updates**

These Onboarding and Offboarding Procedures will be subject to a formal review at least annually. This review will be conducted jointly by representatives from Human Resources, the IT department (including Operations and Helpdesk), and the IT Cybersecurity team. The procedures will be updated as necessary to:

- \* Reflect changes in Bank processes, organizational structure, or technology systems.
- \* Incorporate new or revised regulatory requirements.
- \* Address emerging security threats or vulnerabilities.
- \* Incorporate lessons learned from audits, security incidents, or process inefficiencies.

Approved updates will be documented and communicated to all relevant personnel. *Rationale:* Ensures the procedures remain current, effective, and aligned with the evolving needs and risk environment of World Bank.