

# Mobile and Portable Device Security Policy

## 2.1. Purpose and Scope

This policy establishes the mandatory security requirements for all mobile and portable computing devices, including but not limited to smartphones, tablets, and laptops, that are used to access, store, or transmit World Bank information or connect to World Bank networks. This applies to both bank-owned devices and personally-owned devices (Bring Your Own Device - BYOD) where explicitly permitted under the World Bank BYOD Program. The primary goal is to protect sensitive bank and customer data from unauthorized access, disclosure, modification, loss, or destruction, recognizing that the proliferation and use of mobile devices inherently increase security risks if not properly managed. Adherence to this policy is critical for maintaining the confidentiality, integrity, and availability of World Bank's information assets.

Mobile devices represent a significant endpoint risk due to their portability, connectivity, and the potential to store or access substantial amounts of sensitive data. This policy is designed to enforce robust security measures, drawing from industry best practices, while enabling the productivity benefits these devices offer. It is imperative that the convenience afforded by mobile technology does not compromise the security of the sensitive financial data entrusted to World Bank.

## 2.2. Acceptable and Unacceptable Use Guidelines

All users of mobile and portable devices accessing World Bank resources must adhere to the following use guidelines:

- **Acceptable Use (for Bank-issued and Approved BYOD devices):**
  - Accessing official World Bank corporate email, calendar, contacts, and approved business applications through authorized channels.
  - Securely connecting to the World Bank internal network via the bank-approved Virtual Private Network (VPN) client when outside the bank's physical premises.
  - Storing non-sensitive, work-related files necessary for immediate job functions, provided the device is fully encrypted and compliant with all security requirements herein.
  - Promptly reporting any suspicious activity, potential compromise, loss, or theft of the device to the World Bank IT Help Desk and Security Operations Center (SOC).
  - Utilizing devices for work-related communication (calls, messages, video conferences) in a professional manner, respecting privacy and confidentiality.

- Ensuring the physical security of the device by not leaving it unattended in public or insecure locations.

- **Unacceptable Use:**

- Downloading, installing, or running applications from unapproved or untrusted sources, including third-party app stores not sanctioned by World Bank IT.
- Attempting to "jailbreak" (iOS) or "root" (Android) devices, or otherwise bypassing the operating system's security controls or manufacturer's warranty restrictions.
- Storing sensitive or confidential World Bank data (e.g., customer PII, account numbers, internal strategic documents) on unencrypted personal devices, personal cloud storage accounts, or removable media not explicitly approved and encrypted by World Bank IT.
- Connecting to public, unsecured Wi-Fi networks for accessing or transmitting sensitive World Bank information without an active and functioning bank-approved VPN connection.
- Sharing bank-issued mobile devices with non-World Bank personnel or family members. User accounts and credentials must not be shared.
- Using bank-owned or BYOD devices (while connected to bank resources) for any illegal activities, to harass, threaten, or impersonate others, or to access, store, or distribute offensive, indecent, or obscene material.
- Attempting to circumvent or disable World Bank security measures, monitoring tools, or Mobile Device Management (MDM) configurations.
- Using the device in a manner that could degrade the performance or security of World Bank information resources.
- Leaving devices logged into World Bank systems unattended, especially in non-secure environments.
- Using default or easily guessable passwords/PINs for device or application access.

Clear delineation between acceptable and unacceptable use is fundamental for user accountability and effective policy enforcement. General prohibitions found in information security best practices are translated here into specific, actionable guidelines relevant to World Bank's operational environment. For instance, "downloading unapproved applications" specifically means no third-party financial management apps that haven't been vetted by World Bank IT Security, no games which could harbor malware, and no utilities that might compromise device integrity. This specificity helps employees understand their responsibilities and reduces ambiguity, which is critical for protecting sensitive financial data

processed or accessed via mobile devices. Adherence to the overall World Bank Acceptable Use Policy is also required.

### **2.3. Mandatory Security Requirements**

All mobile and portable devices used for World Bank business, whether bank-owned or approved BYOD, must comply with the following minimum security requirements. These are enforced, where technically feasible, through the World Bank Mobile Device Management (MDM) solution:

- **Strong Passwords/PINs & Biometric Authentication:**
  - Devices must be secured with a strong password or PIN. Minimum password length for laptops is 12 characters, including a mix of uppercase letters, lowercase letters, numbers, and symbols. Minimum PIN length for smartphones/tablets is 6 digits.
  - Passwords/PINs must not be easily guessable (e.g., birthdays, sequential numbers) and must be changed at least every 90 days.
  - Biometric authentication (e.g., fingerprint, facial recognition) must be enabled as an additional security layer where supported by the device and MDM policy.
- **Device Encryption:**
  - Full-disk encryption (e.g., BitLocker for Windows, FileVault for macOS) is mandatory for all bank-issued and BYOD laptops accessing bank data.
  - On-device encryption must be enabled for all smartphones and tablets (iOS and Android) that store or access any World Bank data.
- **Multi-Factor Authentication (MFA):**
  - MFA is required for accessing all World Bank systems, including corporate email, VPN, and sensitive business applications, from any mobile or portable device. Approved MFA methods will be provided by World Bank IT.
- **Remote Wipe Capability:**
  - All devices must be enrolled in the World Bank's MDM solution, which must provide the capability to remotely lock, locate (where legally permissible and appropriate), and wipe all data from the device in the event it is lost, stolen, or compromised.
- **Approved Application List & Controls:**
  - Only applications from an official World Bank approved application list may be installed on bank-owned devices. For BYOD, applications that interact with bank data must be approved.

- The MDM solution may be used to restrict the installation of unauthorized applications or to manage an enterprise app store.
- **Operating System (OS) and Application Updates:**
  - Devices must be configured for automatic download and installation of OS and application security updates. If manual updates are necessary, critical security patches must be applied within 48 hours of release, and other patches within 7 days, unless otherwise directed by IT Security.
  - Devices running unsupported or end-of-life operating systems are prohibited from accessing World Bank networks or data.
- **Secure Wi-Fi Configuration:**
  - Devices must not be configured to automatically connect to unknown or open Wi-Fi networks.
  - Connection to World Bank corporate Wi-Fi must use WPA2/3 Enterprise authentication.
  - Use of the bank-approved VPN client is mandatory when accessing World Bank resources over public or untrusted Wi-Fi networks (e.g., cafes, airports, hotels).
- **Bluetooth Security:**
  - Bluetooth should be disabled when not actively in use.
  - When Bluetooth is enabled, devices should be set to non-discoverable mode unless actively pairing with a trusted device.
- **Anti-malware Software:**
  - Bank-approved anti-malware software with up-to-date signatures must be installed, active, and configured for regular scans on all laptops (bank-owned and BYOD accessing bank networks).
  - For smartphones and tablets, MDM solutions may incorporate mobile threat defense (MTD) capabilities.
- **Session Timeouts & Screen Locks:**
  - Devices must be configured with an automatic screen lock that activates after a short period of inactivity (e.g., 5 minutes for smartphones/tablets, 15 minutes for laptops) and requires re-authentication (PIN, password, biometrics) to unlock.
  - Remote sessions to bank systems must have inactivity timeouts configured.

These mandatory requirements are considered non-negotiable baseline security for any device interacting with World Bank data or systems. The World Bank MDM solution is the primary tool for enforcing these configurations, monitoring compliance, and taking corrective action. For example, the remote wipe capability is a critical control; if a device containing sensitive loan application data is reported lost, security teams must be able to neutralize the threat to that data immediately by wiping the device remotely. This ensures a consistent and enforceable security posture across a diverse range of mobile endpoints.

## **2.4. Incident Reporting Procedures for Lost, Stolen, or Compromised Devices**

Timely and accurate reporting of mobile device security incidents is critical to minimize potential damage and data loss.

- **Immediate Notification Obligation:**
  - Any employee, contractor, or approved BYOD user who loses a device, has a device stolen, or suspects a device has been compromised (e.g., malware infection, unauthorized access attempts) must report the incident immediately.
  - Notification must be made to both the World Bank IT Help Desk and the Security Operations Center (SOC) within a maximum of one (1) hour of discovery of the event. This rapid reporting is crucial for initiating timely response actions.
- **Information to Provide During Report:**
  - Full name and employee/contractor ID.
  - Type of device (e.g., make, model, OS).
  - Whether the device is bank-owned or BYOD.
  - Last known location of the device.
  - Date and time the incident was discovered or occurred.
  - Detailed circumstances of the loss, theft, or suspected compromise.
  - Types of World Bank data potentially stored on or accessible from the device (e.g., email, customer PII, internal documents).
  - Any immediate actions already taken by the user (e.g., attempting to remotely locate).
- **SOC/IT Help Desk Actions Upon Notification:**
  - **Prioritization:** Treat reports of lost/stolen/compromised devices with high priority.

- **Remote Actions:** Immediately attempt to initiate remote lock and/or data wipe procedures via the MDM solution. The decision to wipe versus lock will be based on the sensitivity of data potentially at risk and the likelihood of recovery.
- **Account Actions:** Temporarily disable associated user accounts or restrict access from the affected device if deemed necessary to prevent further unauthorized access.
- **Investigation:** The SOC will initiate an investigation to assess the potential impact, including data exposure or unauthorized system access. This may involve reviewing device logs, network activity, and other relevant security information.
- **Guidance to User:** Provide the user with guidance on next steps, such as changing passwords for associated accounts.
- **User Cooperation:** The individual reporting the incident must cooperate fully with any investigation conducted by World Bank Security or IT personnel.
- **Replacement Device Protocol:** Procedures for issuing a replacement bank-owned device will be followed once the security implications of the incident have been assessed and mitigated. BYOD users may be temporarily restricted from accessing bank resources until their device is secured or replaced.
- **Reporting to Authorities (if applicable):** World Bank Security Management, in consultation with the Legal Department, will determine if notification to law enforcement or regulatory bodies is required based on the nature of the incident and data involved.

The speed of reporting a lost, stolen, or compromised device is paramount. The one-hour timeframe for notification is established because the window of opportunity for an attacker to exploit a lost device can be very short. Prompt reporting allows IT and Security teams to trigger remote security measures like data wipe or device lock swiftly, significantly reducing the risk of sensitive data falling into the wrong hands and mitigating the potential impact of a breach on World Bank and its customers.

## 2.5. User and Bank Responsibilities

Protecting World Bank information on mobile and portable devices is a shared responsibility:

- **User Responsibilities:**
  - Strict adherence to all sections of this Mobile and Portable Device Security Policy and the overarching World Bank Acceptable Use Policy.
  - Maintaining the physical security of any device used for bank business, including safeguarding against loss, theft, or damage.

- Ensuring that all security software (e.g., anti-malware, MDM client) is active, not tampered with, and allowed to receive updates as pushed by World Bank IT.
- Using strong, unique passwords or PINs for device access and for World Bank applications, and protecting these credentials from disclosure.
- Promptly reporting any security incidents, suspected vulnerabilities, or policy violations related to mobile devices as per section 2.4.
- Ensuring personal use of bank-owned devices is minimal and does not interfere with security or compliance requirements.
- Cooperating with IT and Security personnel during device audits, incident investigations, or when security updates are required.
- Securely returning all bank-issued devices and any associated peripherals to World Bank IT upon termination of employment or contract, or when the device is replaced.
- Ensuring any approved BYOD device is removed from MDM and all bank data is securely wiped (if not done remotely by IT) upon cessation of its use for bank business.

- **World Bank Responsibilities:**

- Providing, implementing, and maintaining a robust Mobile Device Management (MDM) solution for centrally managing and securing bank-owned and enrolled BYOD devices.
- Defining, maintaining, and communicating the list of approved applications and configurations for devices accessing bank resources.
- Providing regular security awareness training to all users on the risks associated with mobile device usage, secure practices, and their responsibilities under this policy.
- Implementing and maintaining the necessary backend security infrastructure to support secure mobile access (e.g., VPN gateways, MFA systems, secure email gateways).
- Promptly investigating all reported mobile device security incidents, taking appropriate corrective and preventative actions.
- Conducting periodic reviews and risk assessments of the mobile device environment and updating this policy as necessary to address emerging threats and technologies.
- Ensuring that procedures for device provisioning, de-provisioning, and disposal are secure and documented.

- Providing clear channels for users to report incidents and seek assistance with mobile device security issues.

Security is a collaborative effort. While World Bank provides the technological framework and security policies, the diligence and responsible behavior of each user are critical in forming the first line of defense for their devices and the sensitive information they access. This shared understanding of obligations is essential to the overall security posture of World Bank.

## 2.6. Actionable Items and Examples for Simulation

The following policy statements, procedures, requirements, and scenarios are designed to be directly usable in a cybersecurity simulation environment for World Bank:

1. **Policy Statement:** "All bank-issued laptops must be encrypted using AES-256 bit full-disk encryption, managed via the World Bank MDM solution."
2. **Procedure:** "Employees must report a lost or stolen mobile device (smartphone, tablet, or laptop) to the World Bank SOC via the dedicated incident hotline (ext. 5555) or by emailing soc@worldbank.sim within sixty (60) minutes of becoming aware of its absence."
3. **Example (Unacceptable Use):** "An employee is found to have stored an unencrypted spreadsheet containing customer names, account numbers, and recent transaction details on a personal USB flash drive, which was then connected to their bank-issued laptop." *Simulation Task: What policy violations occurred? What are the potential consequences?*
4. **Requirement:** "Multi-Factor Authentication (MFA) using the World Bank approved authenticator application is mandatory for accessing the bank's VPN from any mobile or portable device."
5. **BYOD Rule:** "Personally-owned devices (BYOD) approved for accessing World Bank email and calendar must be enrolled in the World Bank MDM solution and meet all security requirements outlined in section 2.3 of this policy."
6. **Security Setting:** "All mobile devices (smartphones, tablets) accessing bank data must be configured to auto-lock after a maximum of 5 minutes of inactivity. Laptops must auto-lock after 15 minutes."
7. **Prohibited Software:** "The installation and use of peer-to-peer (P2P) file-sharing applications (e.g., BitTorrent clients) are strictly prohibited on all devices used for World Bank business or connected to the World Bank network."
8. **Incident Scenario (Simulation):** An employee leaves their bank-issued tablet, which contains cached emails and attachments with sensitive project data, in a taxi. They realize it is missing three hours later. *Simulation Task: According to policy, what steps should the employee take immediately? What actions will the SOC initiate?*



9. **User Responsibility:** "Users are responsible for ensuring their device's operating system and all installed applications are updated with the latest security patches within 72 hours of official release by the vendor, unless these updates are managed centrally by World Bank IT via MDM."
10. **Bank Responsibility:** "World Bank IT will conduct quarterly automated compliance checks via the MDM solution for all enrolled devices against the mandatory security requirements of this policy. Non-compliant devices may have access to bank resources restricted."
11. **Acceptable Use Example:** "Using a bank-issued, encrypted laptop to conduct a secure video conference with a client via the World Bank approved and hardened video conferencing platform, while connected to a trusted, secured Wi-Fi network."
12. **Password/PIN Rule:** "Mobile device PINs must be at least 6 digits. Laptop passwords must be at least 12 characters. Neither must contain easily guessable patterns (e.g., '123456', 'password123', username, or bank name)."
13. **Remote Wipe Trigger Condition:** "A remote wipe of a device will be initiated by the SOC if the device is reported stolen and cannot be located via MDM within 4 hours, or immediately if it is known to contain highly sensitive (Level 3 or 4) World Bank data and the risk of compromise is high."
14. **Training Point (Simulation Material):** "A training module will cover how to identify and report smishing (SMS phishing) attempts targeting mobile devices and requesting World Bank credentials."
15. **Unacceptable Use Example:** "Connecting a bank-issued laptop to an unknown, unsecured public Wi-Fi network (e.g., at a public event) to access internal World Bank file shares without using the corporate VPN." *Simulation Task: Identify the policy violation and the associated risks.*
16. **Procedure:** "Before an employee disposes of an old personal mobile device that was previously used for approved BYOD access, they must ensure it is unenrolled from World Bank MDM and that all bank-related data and applications have been securely removed, as verified by IT if necessary."
17. **Security Setting:** "The use of third-party cloud storage services (e.g., personal Dropbox, Google Drive) for storing any World Bank documents or data on mobile devices is strictly prohibited, unless the service is an officially approved and secured World Bank platform."
18. **Policy Enforcement:** "Violation of this policy may result in disciplinary action, up to and including termination of employment or contract, in accordance with World Bank HR policies and legal agreements. Access to bank resources from non-compliant

devices may be automatically blocked by the MDM or network access control systems."

**19. Requirement:** "Users must not disable or tamper with any security software or configurations deployed by World Bank IT, including MDM profiles, anti-malware agents, or encryption settings."

**20. Acceptable Use (BYOD):** "Approved BYOD devices may be used for incidental personal tasks, provided such use does not violate any World Bank policies, introduce security risks, or consume excessive resources that impact work performance. However, World Bank data must remain segregated and protected."

## 2.7. Table: Mobile Device Security Configuration Checklist

This table provides a practical checklist for verifying the security configuration of mobile and portable devices at World Bank. It translates policy requirements into specific, auditable settings, which is essential for both users ensuring their compliance and IT/Security teams performing checks or responding to incidents. This is a key tool for simulation exercises where students might need to assess device security posture.

Security Setting/Control	Required Configuration for World Bank Devices	Verification Method (How to check if compliant)	MDM Enforcement Capability
<b>Device Passcode/Password</b>	Min. 6-digit PIN (Mobile), Min. 12-char complex password (Laptop). Changed every 90 days.	Check OS settings for passcode/password policy compliance; MDM console.	Yes
<b>Biometric Authentication</b>	Enabled (Fingerprint/Facial Recognition) if device supports it, as an additional layer.	Check OS security settings; MDM console.	Yes (Enable/Require)
<b>Device Encryption</b>	Full Disk Encryption (Laptops: BitLocker/FileVault), On-Device Encryption (Mobiles: iOS/Android native) Enabled.	Check OS encryption status (e.g., manage-bde -status on Win, System Settings on macOS/iOS/Android); MDM console.	Yes
<b>Multi-Factor Authentication (MFA)</b>	Required for all access to World Bank corporate resources (email, VPN, apps).	Attempt login to corporate resource from device; check user's MFA enrollment status in identity provider.	Partial (MFA for apps)
<b>Remote Wipe Capability</b>	Device enrolled in World Bank MDM with remote wipe function confirmed active.	MDM console shows device enrolled and "Wipe" command available/tested.	Yes
<b>Operating System Version</b>	OS must be within N-1 version of the latest stable release from vendor; No End-of-Life OS.	Check OS version in device settings; MDM inventory report.	Yes (Compliance Policy)
<b>OS &amp; App Patching</b>	Critical patches applied <48hrs, others <7days. Auto-updates enabled where possible.	Check patch levels/update history in OS settings; MDM compliance report.	Yes (Push/Schedule)

<b>Approved Applications Only</b>	No unauthorized apps installed (Bank-owned). Approved apps only for bank data access (BYOD).	Review installed applications list against approved list; MDM app inventory/blacklist.	Yes (App Control)
<b>Anti-Malware Software (Laptops)</b>	World Bank approved anti-malware installed, active, real-time protection enabled, definitions up-to-date.	Check anti-malware client GUI for status; MDM endpoint security status.	Yes
<b>Mobile Threat Defense (Mobiles)</b>	MDM-integrated MTD solution active and reporting.	MDM console for MTD status and threat alerts.	Yes
<b>Secure Wi-Fi Configuration</b>	Corporate Wi-Fi profile (WPA2/3 Enterprise) installed; No auto-connect to open networks.	Review Wi-Fi network profiles on device; MDM configuration profiles.	Yes (Profile deployment)
<b>VPN Client</b>	World Bank approved VPN client installed and configured. Mandatory for public Wi-Fi access to bank resources.	Check for VPN client installation and configuration profile; test VPN connectivity.	Yes (App deployment)
<b>No Rooting/Jailbreaking</b>	Device integrity check confirms OS has not been rooted (Android) or jailbroken (iOS).	MDM console device integrity status; specific detection apps.	Yes (Detection/Alert)
<b>Screen Lock Timeout</b>	Max 5 mins (Mobiles), Max 15 mins (Laptops) inactivity before auto-lock.	Check OS screen lock settings; MDM policy.	Yes
<b>Bluetooth Security</b>	Disabled when not in use; Non-discoverable mode when active.	Check Bluetooth status and settings.	Partial (Some MDMs)
<b>Camera/Microphone Restrictions</b>	Restrictions on camera/microphone use by certain apps or in certain geofenced areas (if MDM supports).	MDM policy configuration; test app permissions.	Yes (If MDM supports)
<b>Data Loss Prevention (DLP)</b>	MDM policies preventing copy/paste to unmanaged apps, or blocking unapproved cloud storage.	Test DLP rules (e.g., try to save corporate data to personal cloud drive); MDM policy.	Yes