# Mobile Device Management (MDM)

|  |  |
| --- | --- |
| Revision | 1.0 |
| Approval | Pending |

Securely provision, monitor, and manage mobile devices used for business purposes. Prohibit the use of unauthorized mobile devices.

#### Commentary

The National Institute of Standards and Technology (NIST) defines a "mobile device" as:

"A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source."

For the purpose of this policy, the following items are considered to be "mobile devices."

* Laptops
* Phones (e.g., smartphones, cellphones, etc.)
* Tablets
* Wearables (e.g., smartwatches, smart glasses, etc.)
* Other portable devices (e.g., e-readers, digital assistants, navigation devices, digital cameras, etc.)

The use of mobile devices for business purposes is becoming more common due to technological advancements and operational efficiencies. Some examples of mobile device use for business purposes could include, but are not limited to:

* Connecting to the organization's network from a remote location (a.k.a., "remote access").
* Performing remote processing functions.
* Building resilience into business continuity objectives.
* Accessing, storing, or transmitting organization or customer information.
* Using work communication channels, like email, team collaboration tools, video conferencing, or file sharing.

To promote security, the organization needs to ensure effective mobile device controls are in place, and users are educated on security expectations.

At times, personnel may wish to use a personally-owned device to perform work-related duties. This is commonly referred to as "bring your own device" or "BYOD." If the organization elects to allow BYOD, the same security requirements for both organization-owned and personally-owned mobile devices should be enforced. BYOD devices are inherently less standardized than organization-owned devices and therefore may require additional inspections outside of the normal assurance and testing process.

#### Implementation

Implement a process to provision, monitor, and manage mobile devices used for business purposes.

* Require senior management to perform due diligence and approve mobile devices for use. Approval can be granted or revoked based on factors including, but not limited to, specific types of devices; data to be accessed by the device; encryption levels; use cases or job functions; specific users; changes in technology; and/or other relevant risk factors.
  + Document approved mobile devices in the IT asset inventory, including personally-owned mobile devices.
* Review approved mobile devices on a periodic basis to determine if the status of any approvals needs modified or revoked.
* Use a mobile device management (MDM) system to centrally administer mobile devices.
* Retain the authority to audit authorized mobile devices.
* Prohibit the use of unauthorized mobile devices on the organization network. Monitor for use of unauthorized mobile devices in accordance with organization policy (see the "Related Policies" section for details).
* Communicate mobile device expectations to personnel in the Acceptable Use Policy (AUP). Train personnel on risks and considerations related to mobile device use.
* Follow organization policy to decommission mobile devices which have reached end-of-life (EOL) or can no longer be used by the organization (see the "Related Policies" section for details).

**Secure Configuration**

Before a mobile device is allowed to be used, whether organization-owned or personally-owned, inspect the device.

Ensure the device is configured to:

* Require authentication prior to accessing information on the device (e.g., password, passcode, biometrics, etc.).
* Lock after a period of inactivity.
* Remote wipe.
* Lockout or automatically erase the device after failed logon attempts.
* Encrypt data at rest and in transit.
* Install patches and updates (e.g., OS updates, app updates, etc.).

In addition, verify the device:

* Is not modified in a way that could circumvent security controls (e.g., jailbreaking, rooting, etc.).
* Has anti-malware installed, when possible.
* Only uses applications downloaded from reputable stores authorized by the device manufacturer (e.g., Apple's App Store, the Google Play Store, the Microsoft Store, etc.).
* Is configured to pair only with known Bluetooth devices.
* Has an approved virtual private network (VPN) configured, if necessary.

Validate the mobile device’s patch status and require the device to be up to date before allowing it to connect to the organization network.

**Mobile Device Reset**

When possible and in accordance with the organization's Incident Response Plan, disable, remote wipe, and/or factory reset any mobile device which is:

* Reported to be lost or stolen.
* Believed to be compromised or breached.
* Infected by malware.

**Termination Considerations**

As part of personnel termination procedures:

* **For organization-owned mobile devices,** reclaim the device. When appropriate and after the organization has been able to obtain any information needed from the device, perform a factory reset and follow organization policy to reconfigure the device (see the "Related Policies" section for details).
* **For personally-owned mobile devices:**
  + Remove any organization or customer data from the device.
  + Perform an assessment to determine if the device needs a factory reset. Consider the following:
    - Data the employee was authorized to access and/or use on the device.
    - If network or data access can be restricted in another way (e.g., account deactivation).
    - The risk of future unauthorized access to or misuse of residual data on the device.
    - Any personal data which may be lost by a reset (e.g., photos, documents, etc.). If a reset is required, determine if there is another way to preserve personal data.
    - Other types of risks associated with resetting a former employee's mobile device (e.g., legal risks, reputation risks, etc.).
  + Determine if the organization needs to reclaim any assets related to the device (e.g., phone number, service plan, etc.). If the organization paid for the mobile device's service plan, contact the carrier to update the plan.

#### Implementation Responsibility

* Network Administrator

#### Related Policies

| Related Policy | Description |
| --- | --- |
| Data Management | Decommission mobile devices in accordance with this policy. |
| Employee Security Awareness Training | Include mobile device security in security awareness training. |
| Incident Management | Ensure the Incident Response Plan addresses possible mobile device incidents (e.g., lost or stolen mobile devices, compromised devices, mobile malware, etc.). |
| IT Asset Management | Document mobile devices on the IT asset inventory. Monitor for the use of unauthorized mobile devices (a.k.a., “shadow IT”) in accordance with this policy. |
| Personnel Security | Address mobile devices as part of personnel termination procedures. |
| Remote Access | Ensure mobile devices authorized for remote access comply with this policy. |
| Security Testing | Periodically audit authorized mobile devices. Identify unauthorized mobile devices connected to the network as part of vulnerability assessments. |
| System Hardening | Ensure both new and refurbished mobile devices are securely configured. Consider using profiles (e.g., Apple Configuration Profiles, Android Work Profiles, etc.) to separate work use from personal use on the device. |
| User Authentication | Require authentication to access the mobile device. |
| Vulnerability and Patch Management | Ensure mobile devices are patched in accordance with this policy. |

#### Committee/Team Review Items

| Frequency | Responsibility | Description |
| --- | --- | --- |
| Quarterly | Security Committee | Confirm the IT asset inventory includes mobile devices approved for use since the last meeting. |
| Quarterly | Security Committee | Review mobile devices approved for use. Determine if any approvals need modified or revoked. |
| Semiannually | Audit Committee | Audit a sample of approved mobile devices to determine if they comply with configuration requirements. |
| Semiannually | Security Committee | Review any incident reports related to mobile devices (e.g., lost or stolen devices, compromised devices, mobile malware, etc.). |