|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Standard**:  **Mobile Device Security** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of the Mobile Device Security Policy is to establish comprehensive guidelines for securing mobile devices used within the organization, recognizing that these devices face unique risks due to their portability and connection to various networks. This policy aims to enhance the security posture of the organization by mandating specific protections, such as device encryption, authentication protocols, and approved application usage. By implementing these measures, the organization seeks to safeguard sensitive information accessed or stored on mobile devices, thereby reducing the potential for data breaches and unauthorized access.

Implementing the Mobile Device Security Policy offers several significant benefits. First, it helps protect sensitive organizational data from theft or loss, especially as mobile devices are frequently used in diverse environments. Second, it ensures compliance with regulatory requirements and industry best practices, minimizing the risk of legal repercussions. Third, the policy promotes a culture of security awareness among users, educating them about the risks associated with mobile device usage and the importance of following security protocols. Ultimately, by enhancing mobile device security, the organization can improve overall cybersecurity resilience and maintain trust with stakeholders and clients.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The Mobile Device Security Policy establishes necessary protections for mobile devices that access or store organizational information, addressing the heightened risks associated with their use. This policy applies to all employees, contractors, and third-party vendors, covering both entity-issued and personal devices. It mandates the implementation of encryption, approved applications, authentication protocols, and centralized device management to mitigate security threats. Users are responsible for adhering to these guidelines to ensure the confidentiality, integrity, and availability of sensitive information. Non-compliance may result in disciplinary actions, reinforcing the organization's commitment to safeguarding its information assets.

* 1. Mobile Device Definition

Mobile devices are computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and is portable (i.e., non-stationary). These devices come in the forms such as: smartphones, PDAs, smart watches, tablets, laptops, and wearable devices. Mobile devices must follow all requirements of the Information Security Policy.

* 1. Device Encryption

As per the Encryption Standard, all mobile devices that access or contain any entity information must be encrypted.

* 1. Approved Applications

For entity issued mobile devices or personal mobile devices with direct access to managed networks, only those applications which are approved may be installed and or run on the mobile devices. Applications must be restricted through the use of whitelisting (preferable) or blacklisting. Applications must be digitally signed to ensure that only applications from trusted entities are installed on the device and that code has not been modified.

* 1. Authentication Lockout

Entity information must be removed or rendered inaccessible from mobile devices after no more than 10 incorrect authentication attempts.

* 1. Idle Lockout

Mobile devices must automatically lock after being idle for a period not to exceed 10 minutes.

* 1. Network Access

1. Mobile devices which directly connect to managed private networks, virtually connect to managed private networks in a manner consistent with a directly connected device, or which contain or could contain information, including e-mail data, must be managed by a Mobile Device Management (MDM) or other centralized management solution.
2. Mobile devices may not access private networks unless their operating environment integrity is verified (including whether the device has been rooted/jailbroken).
   1. Device Backups

Use of synchronization services, such as backups, for mobile devices (e.g., local device synchronization, remote synchronization services, and websites) must be controlled through an MDM or other centralized management solution.

* 1. Device Management

The [Owner] shall manage all mobile devices by:

1. Implementing device policies and configurations as appropriate to the use of the device.
2. Developing and implementing processes which check for upgrades and patches to the software components, and for appropriately acquiring, testing, and deploying the updates to entity issued devices.
3. Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.
4. Detecting and documenting anomalies which may indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems’ administrators as appropriate.
5. Providing training and awareness activities for mobile device users on threats and recommended security practices which can be incorporated into the entity’s security and awareness training.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
| Mobile Devices | Computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and is portable (i.e., non-stationary). These devices come in the forms such as: smartphones, PDAs, smart watches, tablets, laptops, and wearable devices. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[NIST Special Publication 800-124, Guidelines for Managing and Securing Mobile Devices in the Enterprise](https://csrc.nist.gov/pubs/sp/800/124/r2/final" \t "_blank)