Idaho Technology Authority (ITA)

ENTERPRISE POLICY P4500 – Security – Computer and Operations Management

Category: P4550 – MOBILE DEVICE MANAGEMENT

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-833

II. ABSTRACT

The purpose of this policy is to ensure that the use of mobile devices does not adversely affect the security of state information.

III. DEFINITIONS

See ITA Enterprise Guideline G105 (Glossary of Terms) for any definitions.

IV. POLICY

This policy applies to mobile devices, state-owned or personally-owned, which accesses the state network, state email, or accesses, creates, modifies, transmits, stores, or views state data classified as Level 2 and above. Exempt from this policy are devices defined as “Internet of Things” (IoT) devices, industrial control systems (ICS), simple mobile and storage devices, and personally owned mobile devices that use State Multifactor Authentication solutions but in no other way meet the applicability criteria of this policy.

Agencies may restrict data types that mobile devices are allowed to store, process, transmit, and receive.

Agencies may be required to define stricter controls to adhere to regulatory compliance or increased risk determined by the sensitivity of the data. Follow ITA Enterprise Guideline G540 (Mobile Devices) for further reference.

Users must sign an Mobile Device User Agreement. Minimum requirements are set in Standard

Mobile devices at a minimum must:

a) Require one or more of the following to unlock the device:
    1) A password or PIN that meet standard S6030 – Identity and Authentication
    2) Biometric (fingerprint, facial scan, etc.)
    3) Authentication pattern
    4) Multifactor Authentication solution
b) Automatically lock screen after no more than ten (10) minutes of inactivity.
c) Use current manufacturer supported operating systems.
d) Include security software that defends against malicious software and regularly scans (recommended weekly) for security issues.
e) Be kept up to date with the latest antimalware definitions, applications, operating system, and firmware.
f) Enforce encryption to the current state standard.
g) Not be jailbroken, rooted, or otherwise gain administrative access that bypasses manufacturer restrictions.

V. EXEMPTION PROCESS

Refer to ITA Enterprise Policy P1010 (Information Technology Policies, Standards, and Guidelines Framework).

VI. PROCEDURE REFERENCE

- ITA Enterprise Standard S2140 (Mobile Device Security Capabilities)
- ITA Enterprise Guideline G540 (Mobile Devices)
- NIST Special Publication 800-183 (Network of 'Things')
- ITA Enterprise Policy P1040 (Employee Electronic Mail and Messaging Use)
- ITA Enterprise Policy P1050 (Employee Internet Use, Monitoring and Filtering)
- ITA Enterprise Policy P4130 (Information Systems Classification)
- ITA Enterprise Guidelines G550 (Cleansing Data from Surplus Computer Equipment)

VII. CONTACT INFORMATION

For more information, contact ITA Staff at (208) 605-4064.

REVISION HISTORY

09/04/25 – It now applies specifically to devices accessing Level 2 or higher classified state data. Authentication requirements have been strengthened, mandating that PINs comply with standard S6030. Agencies are granted greater discretion to restrict the types of data mobile devices can process and to enforce stricter security measures based on compliance needs. Additionally, users are now explicitly required to sign a Mobile Device User Agreement. Encryption is no longer tied solely to sensitive data classification but is enforced as a general requirement. The policy structure has also been revised to give agencies more authority in implementation and enforcement.

05/31/22 – Extended Abstract; moved definitions to G105; defined minimum requirements needed for a mobile device to increase security requirements at four distinct levels.

07/01/18 – Updated Idaho statute references.

05/09/17 – Refined scope definitions in Section III; updated Section IV. Policy; updated Section VI. Procedure Reference.

07/01/13 – Changed “ITRMC” to “ITA”.

Date Established: June 27, 2012