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. This policy defines minimum security requirements for devices based on how the device is used and what information the user accesses, creates, modifies, transmits, or stores, regardless of whether the device is owned by the state or by the user.

III. DEFINITIONS

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

IV. POLICY

This policy applies to any mobile device, state-owned or personally-owned, which accesses the state network, state email, or accesses, creates, modifies, transmits, stores, or views any state data. 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 choose to write stricter interagency policy, and or follow ITA Enterprise Guideline G540 (Mobile Devices) for further reference.

Those devices without capabilities to meet these policies must be replaced by models which can, in accordance with ITA Enterprise Standard S2140 (Mobile Device Security Capabilities).

1. For devices which only connect to basic state services (cloud email: Microsoft M365, O365; Outlook Web Access):

    a. The device must:
        1) Require one or more of the following to unlock the device:
            i. A password or PIN with a minimum of four characters
            ii. Biometric (fingerprint, facial scan, etc.)
            iii. Authentication pattern
            iv. Multifactor Authentication solution
        2) Automatically lock screen after no more than five (5) minutes of inactivity.
        3) Include security software that defends against malicious software and regularly scans (weekly suggested) for security issues.
        4) Keep applications, operating system, and firmware up to date.
        5) Meet the security requirements listed or it is **not** authorized to access basic state services.

    b. The user must:
        1) Ensure the device they use to access basic state services meets the requirements above.
        2) Not jailbreak, root, or otherwise gain unauthorized administrative access to the device.
        3) Notify their IT department within 24 hours if a device used to access basic state services is lost, stolen, or transferred to another user.
        4) Receive agency permission to access basic state services.
        5) Avoid connecting to public Wi-Fi, unless using a state-licensed, always-on global virtual private network (VPN). Connections to public Wi-Fi are not recommended.

    c. The agency must:
        1) Document User Agreements with employees authorized to access basic state services - a sample agreement is provided in ITA Enterprise Standard S2140s (Mobile Device Security Capabilities).
        2) Review the employee User Agreement annually or when duties, position, access requirements, employment status, or other factors make adjusting the User Agreement applicable.

2. For devices which connect to more advanced state services (agency specific business applications, databases, files, or emails that may contain sensitive information in Classification 2 or higher as defined in ITA Enterprise Policy P4130 Information Systems Classification) inside the state network through a VPN or other remote secure connection:

    a. All the preceding requirements for accessing basic state services apply in

addition to those that follow.

b. The device must:
   1) Be configured to automatically purge/wipe data from the device on ten (10) consecutive, unsuccessful logon attempts.

c. The user must:
   1) Work with their IT Support to ensure that their connection to advanced state services is secure.

d. The agency must:
   1) Attach to the employee User Agreement a list of applications and databases authorized for access.
   2) Consider providing (recommended) a state-owned device to the user for accessing more advanced state services.
   3) Maintain an inventory of devices authorized to access or modify state resources or data.

3. For devices which connect to more advanced state services (agency specific business applications, databases, files) inside the state network through a VPN or other remote secure connection while accessing sensitive information, including federally received data, federally regulated data, or other information in **Classification 2** or higher as defined in ITA Enterprise Policy P4130 (Information Systems Classification):

   a. All the preceding requirements for accessing basic or advanced state services apply in addition to those that follow.

   b. The device must:
      1) Support a cryptographic module that is FIPS 140-2 compliant on any device to protect confidentiality and integrity of local data.
      2) Be subject to a Data Loss Prevention Policy.
      3) Meet regulatory requirements if accessing data received from the Federal government.

   c. The user must:
      1) Use a state-owned device.
      2) Not sideload or install apps from sources other than an app store, unless authorized by agency for specific state business requirements.
      3) Not tether to non-state-owned devices.
      4) Not connect to public Wi-Fi, unless using a state-licensed, always-on global virtual private network (VPN).

   d. The agency must:
      1) Provide a state-owned device that meets the security requirements of this policy to the user.

2) Conduct an annual risk assessment of the security controls in place on all devices in the mobile environment. Consult your IT Support.
3) Utilize a device management solution that:
    i. Authenticates devices prior to authorizing access to the state network.
    ii. Logs security events for all devices and the device management server.
    iii. Implements remote protection mechanisms (lock account, purge, or wipe data) in the event a device is lost or stolen.
4) Dispose of all devices following media sanitization and disposal procedures in accordance with ITA Enterprise Guidelines G550 (Cleansing Data from Surplus Computer Equipment)
5) Disable wireless Personal Area Networks that allow a device to connect to other devices via Bluetooth, or near field communication (NFC).
6) Disable to a practical extent, access to hardware, such as the digital camera, global positioning system (GPS), and universal serial bus (USB) interface.
7) Control end user ability to download only authorized applications to the device and must limit the accessibility to Federal data by applications to only authorized applications.
8) Document instances where the agency has authorized a user to install an application source other than the app store.

Any user, to be permitted to use a personally owned mobile device for work purposes must:

a. receive management approval
b. sign an agreement indicating their understanding of the increased responsibilities, as well as the personal and business risks involved in using a personally owned mobile device during state business.
c. Agencies are free to develop a custom agreement for these purposes; however, a sample is provided in ITA Enterprise Standard S2140 (Mobile Device Security Capabilities).

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

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