Tier 1 Control Standards (State-Wide)

Cell Phone & Tablet Use and Access to E-Mail

Standard ID
IOT-CS-SEC-129

Published Date
4/26/2010

Effective Date
4/26/2010

Last Updated
5/17/2017

Next Review Date
5/17/2018

Policy
06.0 Access Control (PR.AC)
06.3 PR.AC-3
06.3.1 Remote Access

Purpose
To set forth the requirements for using cell phones and tablets (e.g. – iPad), and connecting them to the State’s email system

Scope
All Devices that Connect to the State Network

Statement
State Provided Cell Phone and Tablet Usage Requirements:

- Cell phones and tablets provided by agencies to their workforce members are to be used solely to conduct the business of state government with exceptions limited to those provided by State Ethics Rule 42 IAC 1-5-12 and any applicable agency policy.
- Cell phones and tablets, provided by the State as well as any State information stored on such a device, including personal, are defined as “information resources”. Their use is subject to the guidance and restrictions contained in the Information Resources Use Agreement (IRUA).
- Downloading, subscribing to, or accessing music, ringtones, games, or any other chargeable services onto any State provided device is prohibited.
- Sending any communication (e.g. - text, picture, MMS, or video) unless specifically work related on any State provided device is prohibited with exceptions limited to those provided by State Ethics Rule 42 IAC 1-5-12 and any applicable agency policy.
- Cell phone users must be aware of their calling plan restrictions, including minutes available, to appropriately manage use of their cell and landline phones to minimize cost to the State.
- Cell phones and tablets are commonly used outside of the protections afforded by the State of Indiana network. Configuration details and encryption capabilities vary among devices making the security of information stored on these devices uncertain. As such, workforce members are prohibited from storing State information, unless it has been released to the public, on either cell phones or tablets on a lasting basis. Email and calendar information may be stored on these devices only temporarily as dictated by the synchronization process. (For a definition of “State” information, see this link: http://www.ai.org/legislative/ic/code/title5/ar15/ch5.1.html)
- If uncertain whether an activity is permissible, users will refrain from the activity and obtain written authorization from their manager before proceeding.
Personal Cell Phone/Tablet Email Connectivity Security Requirements:

- The Indiana Office of Technology (IOT) will enable connectivity of an individual’s personal cell phone or tablet to the State’s email system upon agency request. Please see Mobile Device Policy for current state standards for mobile devices. (http://www.in.gov/iot/2394.htm)
- Along with agency authorization, the conditions below must be met and agreed to for any device, including personal cell phones and tablets, to connect. IOT will technically enforce the conditions on all cell phones and tablets connected to email. Workforce members should carefully review and consider these stipulations prior to connecting their devices to the State’s email system.
  - All cell phones and tablets, either State provided or personally owned, will require a password with a minimum of 5 characters or 4 characters if an Apple PIN. A change of password is required every 6 months.
  - A 60 minute inactivity period will lock the device, or if possible, the state “compartment” on the device. Users will then be forced to enter their password to access device features.
  - When an individual’s work relationship with the State ends so will their access to the State's email system. Agencies will notify IOT of the need to blank emails from the device. IOT will attempt to wipe only email but cannot guarantee that other data from the individual’s cell phone or tablet will not be lost. Agencies should confirm that users understand this circumstance before they use their personal device to access State email. IOT is not responsible for lost data, contacts, or applications as a result of the wiping process.
  - At an agency’s request, IOT will send a remote command to wipe all data off of a device. Circumstances for such a request would include cell phones or tablets that were lost or stolen, termination of employment circumstances, or other instances where agencies have concerns regarding the security of State information. Those using personal phones devices should be sure to have them backed up regularly.
- Only State provided mobile devices are directly supported by IOT. IOT will provide only basic setup instructions for non-standard devices. Problems connecting personal devices to the State system will need to be resolved between the user, their carrier, and the cell phone or tablet manufacturer.
- After set-up, users experiencing problems receiving state email with their personal devices may contact the IOT Help Desk to review email setup only. IOT will check settings to ensure the problem is not with IOT owned software, hardware and networking. If the problem is not with IOT, the ticket will be closed and the user must seek a resolution with their carrier and the device manufacturer.

Roles
All Personnel

Responsibilities
End users/customers shall accept the responsibility of protecting State information in the form of email messages and attachments accessed via a cell phone. IOT shall enforce security settings on State provided or individually owned cell phones to protect State information in the case of theft or loss.

Management Commitment
Management shall review State provided cell phone billing and call details on a regular basis. Excess personal use may include reimbursement by the employee.

Coordination Among Organizational Entities
Agencies shall notify IOT and report violations of this Standard.

Compliance
IOT will assist agency management to curb abuse by implementing safeguards to stop abuse as requested.

Exceptions
No exceptions.

Associated Links