Office of Information Technology
Policy

Use of Smartphone Devices when Accessing State Networks

Policy:
Smartphone devices that are used to access state email and/or networks, but not including devices that only access email through a web based interface, must have the following security measures enabled: a minimum of a 4 digit PIN is required to access the device; a Group Policy or setting that is pushed down from the email server or wireless enterprise server, which after ten failed login attempts to the device will initiate a complete data wipe ensuring all state data is removed.

A smartphone device includes but is not limited to the following: a personal digital assistant (PDA), a RIM BlackBerry, an Apple iPhone, Windows mobile devices, a Nokia N-Series or any other handheld mobile device with email and web browsing capabilities.

This policy applies to both state owned devices and privately-owned devices that are used to access data owned by the state, including email.

Scope:
All entities under the authority of the Office of Information Technology, pursuant to the provisions of R.S. 39:15.1, et seq., must comply with this policy.

Responsibilities:
All entities that maintain an email server will ensure that the proper settings are enabled on all smartphone devices connecting to their mail server. This can be accomplished by, but not limited to, pushing down a Group Policy from the email/wireless enterprise server to devices establishing connections to these servers.

Owner:
OIT Security Office

Effective Date:
July 27, 2009