



INFORMATION SERVICES

Smartphone/Electronic Device Policy

POLICY Number: C-003

15 February 2013

1. **AUTHORITY:** Director of State Civil Service as contained in La. R.S. 36:54.
2. **REFERENCES:** Office of Information Technology Technical Standard/Procedures: IT POL 1-24 (Use of Smartphone Devices when Accessing State Networks).
3. **PURPOSE:** To state the Director's policy regarding the security of smartphone devices when accessing state-owned email accounts to reduce and/or prevent unauthorized access of State Civil Service data by unintended recipients and/or users. The purpose of such electronic access is to conduct official state business. This policy applies to both state owned devices and privately-owned devices that are used to access data owned by the state, including email.
4. **APPLICABILITY:** This policy shall apply to all employees of State Civil Service.
5. **POLICY:** It is the responsibility of the MIS division to ensure that employees with a smartphone/electronic device used to directly access state email and/or networks are required to have the following security measure enabled: a minimum of a 4-digit PIN required to access the device, which after ten failed login attempts to the device will initiate a complete data wipe ensuring all data is removed.

Employees are responsible for maintenance of the PIN used to access the device. The MIS Division will **not** be able to help in the recovery of lost data as a result of a forgotten PIN.

Those who access the State Civil Service network must notify the MIS Department and sign a form acknowledging that he or she has read the policy and understands what is expected.

A smartphone/electronic device includes but is not limited to the following: an Apple iPad, a tablet PC, 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.

If the device is lost or stolen, the employee must notify the MIS Division immediately. Once notified, the MIS Division will change the user's network password for security purposes.

Please note that this requirement does **not** apply to those who access the state network/email through webmail, but only to those who access the state network/email directly using a smartphone/electronic device.

6. **VIOLATION:** Failure to comply with this policy may result in disciplinary action.
7. **EXCEPTIONS:** The Director of State Civil Service may grant an exception to any provision of this policy, provided such exception shall not be in conflict with Civil Services Rules and Regulations.

s/Shannon S. Templet
Director