BOBBY JINDAL
GOVERNOR

PAUL W. RAINWATER
COMMISSIONER OF ADMINISTRATION

State of Louisiana

Division of Administration
Office of Human Resources

DIVISION OF ADMINISTRATION

POLICY NO. 23

EFFECTIVE DATE: February 1, 2011

SUBJECT: Use of Smartphone Devices for Access to State Data

AUTHORIZATION: _____
Steven Procopio, Appointing Authority

I. POLICY:

It is the policy of the Division of Administration (DOA) to comply with the rules established by the Office of Information Technology's IT Policy 1-24, *Use of Smartphone Devices when Accessing State Networks.* The policy can be located at: http://www.doa.louisiana.gov/oit/pdf/IT_POL_1-24.pdf

Employees are responsible for the security of devices that are used to access State email and/or applications/equipment that are on the DOA network.

The following shall be required of all devices that are governed by this policy, whether they are State or privately owned devices:

- Minimum 4-digit password.
- Maximum security timeout shall be 10 minutes (idle time after which the device will automatically apply a screen lock).
- After 10 unsuccessful password attempts, the wireless device shall be wiped (all data on the device, including personal data, will be erased).
- Device must be compatible with Blackberry Enterprise Server or ActiveSync Enterprise Security Policies.
- Devices which have access to network-connected equipment/data or house State data shall be physically secured by the owner at all times.

Any device that is not capable of maintaining such restrictions shall not be allowed access to State data, including e-mail.

II. PURPOSE:

The purpose of this policy is to protect information technology systems and networks within the DOA.

III. APPLICABILITY:

This policy is applicable to all employees of the Division of Administration in all sections, both general and ancillary appropriations.

IV. RESPONSIBILITIES:

The Appointing Authority is responsible for:

Holding section heads under his supervision accountable for adhering to all aspects of this policy.

Section Heads are responsible for:

Ensuring that each employee under his supervision is made aware of this policy and its contents.

Managers/Supervisors are responsible for:

Ensuring that each employee under his supervision is:

a. made aware of this policy and its contents, as well as any forthcoming revisions.

b. informed that he must abide by the terms of this policy as a condition of employment.

c. informed of the consequences of violating this policy.

Employees are responsible for:

Following all rules outlined in this policy and ensuring that his supervisor is made aware of any lost or stolen device (State or privately owned).

Ensuring security and service compatibility of privately owned devices.

The Office of Computing Services is responsible for:

Pushing down a Group Policy to connected devices to mandate password protection of devices.

V. VIOLATIONS:

Employees found to have violated this policy will be denied access to State data via Smartphone devices and may be subject to disciplinary action up to and including termination.

VI. EXCEPTIONS:

Requests for exceptions to this policy shall be justified, documented and submitted to the Appointing Authority for consideration.