

State of Vermont

Mobile Device Policy



Date:

Originally Approved:

Approved by:

Policy Number:

11/20/12
[Signature]
Deputy

Contents

1.0 Introduction	3
1.1 Authority	3
1.2 Purpose	3
1.3 Scope	3
2.0 Policy	3

1.0 Introduction

1.1 Authority

The Department of Information and Innovation (DII) is authorized “to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government.” See 22 VSA §901(1).

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff. Each must ensure this policy (1) satisfies each agency’s and/or department’s legal requirements, and (2) that its data requirements can be effectively performed by State employees. If applicable State laws or regulations require more stringent requirements, each agency must adopt its own policy explicitly stating the more stringent legal requirements. Agencies shall not develop an internal policy that lowers the minimum requirements listed in this policy.

1.2 Purpose

The purpose of this policy is to protect State of Vermont data and ensure the availability of State computing resources by providing requirements for the appropriate use and configuration of mobile devices.

1.3 Scope

This policy applies to all mobile devices provided by the State, as well as all personal devices that are used to access or store State of Vermont information and/or data that is protected under federal or state regulation, statute or law.

2.0 Policy

Individuals who choose to use personally owned devices to access and/or store protected State information are subject to this policy, are required to sign the “Personal Mobile Device Access Form” located at (http://dii.vermont.gov/Policy_Central), and to submit the form to the DII Security Office prior to accessing systems that may contain protected data. Agencies/departments are responsible for documenting appropriate procedures for use of personal devices.

Mobile device passwords must meet the requirements of the User Password Policy. (http://dii.vermont.gov/Policy_Central).

All mobile devices will have a lock time set after a maximum of ten minutes of inactivity. If an agency or department determines that a shorter time period is required, they are responsible for documenting that requirement.

All mobile devices that access State of Vermont data protected by federal or state regulation, statute or law must be fully encrypted. If a device does not support encryption, that device will not be used to access such data.

Non-state supported cloud services must not be used for any storage or duplication of state data protected by federal or state regulation, statute or law.

The loss or theft of mobile devices must be immediately reported to IT management. Lost or stolen devices will have data remotely wiped by the appropriate department/agency IT staff. Agencies/departments are responsible for documenting appropriate procedures for such actions.

Employees must immediately report any incident or suspected incident of unauthorized data access and/or data loss to their immediate supervisor and IT manager.

In order to protect confidential state information, the State of Vermont reserves the right to forensically audit or wipe, at any time, any mobile device used for State business. The State will not intentionally wipe a personal device without a security concern, but accidental erasure is also possible..

State owned devices must be returned to the agency/department upon employee termination with the agency/department or at device end-of-life.