

Policy on Using Network Capable Mobile Computing Devices to Store or Access Secured State Information

August 8, 2012

DTS Technology Policy 4300-0030

Status: Revision Approved

Effective Date: October 1, 2010

Next Review Date: August 2013

Sponsor: ARB

Approved By: ARB

Introduction

Tablets, and other mobile computing and communication devices have become very popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognized and addressed to protect both the physical devices and the information they contain.

The most effective way to secure confidential data is **not to store it on mobile devices**. As a matter of policy and best practice data should always be secured where it resides. This can be accomplished by storing sensitive data only on secure State approved services and accessing them remotely using secure communication technologies.

State business requirements may, on occasion, justify storing confidential data on mobile computing devices. In these cases, users are required to assure that steps have been taken to keep the data secure. It is the responsibility of the user to recognize these risks and take the necessary steps to protect and secure their mobile computing device.

With the increasing use of smart phones, tablets, and other mobile devices it is necessary to establish a policy governing the use of these devices to store or access State information. This policy is applicable to all such devices whether purchased by the State or purchased by employees for both State and personal use.

Purpose

This policy is necessary to protect the confidentiality, availability, and integrity of State of Utah secured information while stored, transmitted, or processed on mobile computing devices. This policy is not applicable to State data and information that is available on State public Internet sites.

Scope

This policy applies to any mobile computing device that is used to store or access secured State information and has the capability to connect to State network resources. This policy will not supersede any other existing State developed policies but may introduce more stringent

ARB Approved 8.8.12

requirements than current policies dictate. The policy is applicable to all mobile devices, whether purchased by the State or personally purchased, and used by State employees for access to State information and networks. The intent of the policy is to enforce and control access to State resources irrespective of the type of device.

Policy

Any mobile computing device, excluding laptops, accessing or storing State restricted/confidential or internal information is subject to all State security policies and in addition, will adhere to the following. **If the capability exists for the device**, mobile computing devices will be configured or otherwise agree to:

1. Connect to restricted/confidential or internal data through State networks using the security protocols required by DTS. This may include use of secured network connections and use of State approved Virtual Private Network (VPN) services.
2. Receive and install security and other operating system updates from the operating system vendor.
3. Use a device and/or screen saver password. Portable computing devices must, at a minimum, be password protected in accordance with State security policies.
4. Be identified as an approved device on State Networks. Personally owned devices connecting to State secured networks will be registered using the approved DTS mobile computing device registration process within the UMD. Re-registration may be required periodically at the discretion of DTS and by the owner of the device when it is changed or physically updated.
5. Agree that DTS may restrict the access of any mobile computing device to secured State networks if the mobile computing device presents a probable and demonstrable threat to the integrity of State data or other computing resources.
6. Users of **personally owned** mobile computing devices that are registered to connect to secured State network and computing resources agree to:
 - a. Allow the State access, for discovery purposes, to the content stored on the device;
 - b. Give the State the right to remotely disable or wipe the content of the mobile device in the event the device is lost or stolen.
 - c. Not require State support services for the personally owned mobile computing device;
 - d. Pay the approved rate for synchronization of email, contact, and calendar services. The rate may be paid by the agency as deemed appropriate; and
 - e. Hold the State harmless for any damage to the device or its operating system and related software as a consequence of using State secured network or other

ARB Approved 8.8.12

computing resources.

Definitions

A *mobile computing device* is any type of device that is designed to be moved, excluding laptops, which are covered under other policies and guidelines, and is capable of collecting, storing, transmitting, or processing electronic data or images. Movement in this case refers to the device generally not having a fixed connection to the network. Examples of mobile computing devices include, but are not limited to a tablet (e.g iPad), iPhone, Blackberry, Smartphone, or mobile network connected storage device.

The State Network is inclusive of the wired and secured wireless network (e.g. UWDN), and approved agency specific secured wireless networks. Public network resources (e.g. CapNet, and other external wireless networks) are excluded as a secured network resource and must only be used for secure access using VPN services. To gain access to the secured State Network, the device must be registered within the Utah Master Directory (UMD) using the UMD login screen. The user's NetID and password credentials and such other information as may be required by DTS must be provided. Devices must be provisioned for access to secured wireless network and VPN services.

Confidential information includes any individually identifiable information about State of Utah employees, citizens, or others who do business with the State, and such other information designated as confidential under the provisions of the Government Records and Management Act (GRAMA), and other applicable Federal laws and rules. Applicable State security and confidential information policies include the Information Protection 5000-1700, and Confidential Information 5000-1701 policies.

Enforcement

Individuals using mobile computing devices that connect to, or are attached to State network resources, shall abide by the rules of this policy. Any person found to be in violation of this policy will be subject to appropriate disciplinary action as defined by current State policies.

Implementation

This policy will become effective on October 1, 2010. Agencies will be expected to be compliant by December 31, 2010.

Authority

The Department of Technology services is charged in Utah Code 63F-1-104 et seq with the overall responsibility for defining technology standards and policies. The Chief Information Officer (CIO) has rulemaking and policy making authority for technology standards and practices for the Executive Branch agencies as specified in Utah Code 63F-1-206 et seq, with the exception of those agencies exempted in Utah Code 63F-1-102.

References

State Acceptable Use Policy

5000-1700 Information Protection

5000-1701 Confidential Information

5000-1100-S4 Encryption Standards

5000-1100-S5 Portable Computing Devices Security Standard

5000-1400 Identification & Authentication Policy

5000-1400-S1 Identification and Password Standards