

COUNCIL ~ VOTE SLIP

Date: **SEP 14 2010**

	Absent	Motion	2 nd	Aye	Nay	Abstain
Council Member RANDY HORIUCHI				/		
Council Member JENNY WILSON				/		
Council Member JIM BRADLEY		/		/		
Council Chair JOE HATCH				/		
Council Member MICHAEL H. JENSEN	/					
Council Member DAVID WILDE	/					
Council Member JANI IWAMOTO			/	/		
Council Member <i>Steve DeBry</i>	/					
Council Member MAX BURDICK				/		

Other Action:

app

13.1-13.4

SALT LAKE COUNTY
COUNTY-WIDE POLICY
ON
INFORMATION TECHNOLOGY SECURITY
MOBILE DEVICE PROTECTION

Purpose -

The objective of this policy is to protect County agency data stored on County issued mobile devices and to prevent the theft or loss of County issued mobile devices.

Reference -

The policy and standards set forth herein are provided in accordance with Section 3.10 of Countywide Policy 1400, which directs Salt Lake County Information Services to provide security systems and policies. Also reference the following:

- Countywide Policy 1304 - Discovery and Reporting of Wrongdoing or Criminal Activity
- Countywide Policy 1035 - Employee use of Cellular Phones
- Countywide Policy 1400-1 – IT Security Acceptable Use Policy
- Countywide Policy 1400-4 - IT Security Incident Reporting
- Salt Lake County Ordinance – Section 2.81 Security of Personal Identifiers
- Salt Lake County Ordinance – Section 2.82 Records Management

1.0 Scope

All Salt Lake County employees, contractors, consultants, volunteers, and others with a business association with Salt Lake County shall adhere to this policy insofar as they use any County issued mobile device.

2.0 Definitions

Information Technology Resource(s) and/or System(s) (IT resource(s) and/or system(s))

Computers, hardware, software, data, storage media, electronic communications (including, but not limited to, e-mail, fax, phones, phone systems and voice mail), networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access, beyond ordinary public access to, the County’s shared computing and network infrastructure.

County Agency Data

Written, printed or electronic information for County purposes, including numbers, text, images and sounds, which are created, generated, sent, communicated, received by and/or stored on County IT resources or systems. Data does not include hardware, platforms, software, applications or middleware.

Mobile Device

Laptop computers, cell phones, PDA’s, flash drives, or any other portable device capable of storing data.

Logical Security Measures

Any security option available to lock out unauthorized use of a mobile device. Such options are found in the software or operating system on the mobile device. Examples might include screen saver passwords or keypad locks.

Physical Security Measures

Any security option available to limit visibility of and prevent unauthorized physical access to a mobile device. Such options might include a locking compartment, vehicle trunk, locking file cabinet, or locked office door.

3.0 Policy Statement

Any County issued mobile device used to store County agency data shall be properly secured using the following methods:

- 3.1 All County issued laptop computers shall be in compliance with the following:
 - 3.1.1 All hard drives in County issued laptop computers shall employ whole disk encryption.
 - 3.1.2 Encryption keys for whole disk encryption must be stored on a centralized server as approved by County Information Services.
 - 3.1.3 Users of laptop computers shall employ physical and logical security measures.
- 3.2 Users of any unattended County issued mobile device actively connected to any County network shall employ physical and logical security measures.
- 3.3 County agency data stored on any County issued mobile device shall be protected with encryption.
- 3.4 Users of County issued mobile devices shall employ physical and logical security measures.
- 3.5 County Agency data stored on any mobile device not issued by Salt Lake County will be the responsibility of the owner of the mobile device.

4.0 Exceptions

- 4.1 Other exceptions to this policy shall be approved in conformance with Countywide Policy 1001 - Policy Implementation Procedure.

5.0 Enforcement


Anyone found to have knowingly violated this policy shall be subject to disciplinary action, including but not limited to temporary loss of network connectivity, loss of Internet access, or complete and permanent termination of access to any Salt Lake County network; and can lead to other disciplinary action up to and including dismissal from County employment.

6.0 Education

Training will be provided to County employees on this policy.

APPROVED and ADOPTED this 14th day of September, 2010.

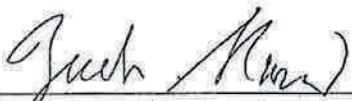
SALT LAKE COUNTY COUNCIL

By: 
JOE HATCH, Chair

ATTEST:


Salt Lake County Clerk

APPROVED AS TO FORM:


Deputy District Attorney
Date: 8-25-10