SALT LAKE COUNTY
COUNTY-WIDE POLICY
ON
INFORMATION TECHNOLOGY SECURITY
INFORMATION TECHNOLOGY SECURITY INCIDENT REPORTING

Purpose -

The purpose of this policy is to ensure that all information technology security incidents are properly reported and responded to in a timely manner.

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 1100 - Surplus Property Disposition/Transfer/Internal Sale
Countywide Policy 1304 - Discovery and Reporting of Criminal Wrong Doing
County Ordinance - 3.36.020 Disposal of property authorized when—Procedures
County Ordinance - 3.36.030 Personal property

1.0 Scope

All Salt Lake County employees and contractors, consultants, volunteers, and others with a business association with Salt Lake County shall adhere to this policy insofar as they use IT resources and systems owned or leased by Salt Lake County or any device that connects to any Salt Lake County network or resides at a Salt Lake County facility.

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 Management
With respect to their own individual offices or departments, any of the following, or their designees: County Mayor, County Executive Branch Department Directors, County Elected Officials, or the County Council as a whole.

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.

Information Technology Security Incident
An information technology security incident is any act with the potential to: adversely affect the integrity or availability of county agency data or a County IT resource or system, provide unauthorized access to any County IT resource or system, or allow a County IT resource or system to be used to launch attacks against the resources and information of other individuals or organizations.

3.0 Policy

All County employees and others with a business association with Salt Lake County shall report information technology security incidents. Examples of information technology security incidents include but are not limited to the following:

3.1 The loss or theft of a County IT resource or system;
3.2 The loss or theft of County agency data;
3.3 The unauthorized or improper alteration of County agency data;
3.4 Any successful or unsuccessful attempt to gain unauthorized access to a County IT resource or system;
3.5 Any successful or unsuccessful attempt to gain unauthorized access to County agency data;
3.6 Any violation of County IT security policy;
3.7 Any unauthorized request or attempt to obtain usernames or passwords;
3.8 Any receipt of a suspicious, threatening or malicious e-mail;
3.9 Any performance issue with a County IT resource or system that gives reason for concern;
3.10 Any unsolicited or suspicious pop-ups, software downloads or software installations;
3.11 Any unauthorized disposal of a County IT resource or system containing County agency data. County IT resources or systems that contain County agency data and that appear to have been improperly disposed of shall be secured until their status can be determined;
3.12 Any activities or events that give reason for concern regarding IT security.

4.0 Reporting an Information Technology Security Incident

All information Technology security incidents shall be immediately reported to Information Services.

In addition to the above notification procedures, employees shall inform their County agency management and their respective department IT Security Advisory Committee representative. County agency management should also reference Countywide Policy 1304 “Discovery and Reporting of Wrongdoing or Criminal Activity.”

5.0 Exceptions

5.1 Exceptions to this policy shall be approved in conformance with Countywide Policy 1001 – Policy Implementation Procedure.

6.0 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.

7.0 Education

Training will be provided to County employees on this policy.

APPROVED and PASSED this 14 day of September, 2010.

SALT LAKE COUNTY COUNCIL

_____
Joe Hatch, Chair

ATTEST:

_____
Sherrie Swensen, County Clerk

APPROVED AS TO FORM:

_____
Deputy District Attorney Date