SALT LAKE COUNTY
COUNTY-WIDE POLICY
ON
VIRUS PREVENTION

Purpose -

This policy is designed to ensure that IT resources and systems owned by Salt Lake County employ effective anti-virus and anti-malware detection software; that IT resources and systems owned by Salt Lake County are free from viruses and malicious code; and, that Salt Lake County will monitor and enforce compliance with this policy. The objectives of this policy are to mitigate risk by effectively managing security exposure or compromise of IT resources and systems; eliminate viruses, worms, and trojan horses and other malware programs that can cause significant damage to IT resources and systems; prevent the destruction, alteration, or disclosure of Salt Lake County information; and, prevent damage to the reputation of Salt Lake County and of the individuals associated with Salt Lake County.

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.

1.0 Scope

The scope of this policy includes any device capable of propagating malicious code and that is used by any employee of Salt Lake County or attached to any Salt Lake County network by wired, wireless, or VPN connection.

2.0 Definition

Information Technology Resources and Systems (IT resources and systems)
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).

3.0 Policy Statement

Any County IT resource or system capable of independently propagating malicious code must have approved anti-virus and anti-malware software installed, updated, and activated as specified by County Information Services.

3.1 All devices will use the County standard virus prevention software as determined by County Information Services. Please refer to the "Recommended Configurations" documentation found on the Information Services Intranet site.

3.2 Virus prevention software must be configured to start automatically when the device powers up.

3.3 Virus prevention software must have up-to-date signatures, and will be configured to update automatically on a timely basis.

3.4 Virus prevention software will be configured for "on access" scanning, where a file is scanned for viruses before an application is allowed to access the file.

3.5 Employees will not do anything to disable or hinder the operation of any virus prevention software.

3.6 In order to prevent virus propagation, no executable software, regardless of the source, will be knowingly loaded on a device connected to any Salt Lake County network without prior approval of the County agency management that owns the device.

3.7 All non-County computing devices, especially laptop computers, must be checked by County Information Services staff before they will be allowed on any Salt Lake County network.

3.8 County Information Services will provide for the installation and maintenance of virus prevention software as a part of Salt Lake County domain membership.

3.9 Employees using Apple, UNIX or LINUX computers will need to contact County Information Services to determine how they can comply with this policy.

4.0 Exceptions

4.1 Devices connected to any Salt Lake County "Guest" network (a network provided strictly for the convenience of the public) are exempt from this policy.

4.2 Any exceptions to this policy must be explicitly approved in writing by County Information Services and shall be approved in conformance with Countywide Policy 1001.

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.

APPROVED and ADOPTED this 24 day of February, 2009.

SALT LAKE COUNTY COUNCIL

_____

Joe Hatch, Chair

ATTEST:

_____
Sherrie Swensen, County Clerk

APPROVED AS TO FORM:

_____
District Attorney's Office Date