

SALT LAKE COUNTY
COUNTY-WIDE POLICY
ON
**INFORMATION TECHNOLOGY SECURITY:
ACCEPTABLE USE POLICY**

Purpose –

This policy is designed to ensure: that IT resources and systems owned by Salt Lake County are used efficiently and appropriately; that Salt Lake County employees and others are aware of the acceptable use of IT resources and systems; that Salt Lake County will monitor the use of IT resources and systems; and, that Salt Lake County will monitor and enforce compliance with this policy. **County IT resources and systems are for County business use only unless specifically stated otherwise in this Policy.**

The objectives of this policy are to mitigate risk by: effectively managing security exposure or compromise of County IT resources and systems; communicating the responsibilities of each County employee for the protection of County IT resources and systems; preserving management's options in the event of an information asset misuse, loss or unauthorized disclosure; and, promoting and increasing the awareness of County employees regarding information security.

Reference –

The policy and standards set forth herein are provided in accordance with Section 3.10 of County-wide Policy 1400, which directs Salt Lake County Information Services to provide security systems and policies. The policy and standards set forth herein are subject to Human Resources Policy "Standards of Conduct," 5702; "Sexual Harassment," 5730; "Discrimination and Reprisal," 5740; and other applicable policy and procedure.

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).

3.0 Policy Statement

It is the policy of Salt Lake County that IT resources and systems are valuable government resources that must be used efficiently and appropriately to carry out the business of Salt Lake County. Salt Lake County will monitor and enforce this policy to ensure that its employees and other users do not use IT resources and systems for impermissible personal uses or for any other uses that violate this policy. County agency management shall implement practices and procedures that promote compliance with this policy. County agency management may adopt more restrictive practices than this policy based on business requirements.

3.1 County Business Use of County IT Systems and Resources.**3.1.1 County IT Resources and Systems are Property of the County, not the User.**

County IT resources and systems are provided for County business purposes only. No County IT resource or system or information contained therein may become the private property of any system user. The County owns all legal rights to control, transfer, or use all or any part or product of its IT resources and systems. Employee e-mails, internet messages, faxes and voice mails are County property subject to County monitoring, control, transfer or use despite any designation as confidential by the sender or recipient. Employees have no reasonable expectation of privacy in electronic communications sent to/from or stored on County IT resources or systems, and County reserves the right to preserve, review, and disclose any such electronic communications without prior notice in the case of litigation, GRAMA requests, to protect the County's interests or comply with applicable laws. Passwords are the property of the County and should not be shared except as appropriate. Users shall comply with public records retention laws and rules.

3.1.2 Access and Control.

Salt Lake County reserves and exercises all rights relating to all information assets. County agency management is responsible for granting users' access to IT resources and systems, which is limited to that which is required to do their work, and for revoking user access in a timely manner. County agency management may withdraw permission for any or all use of its IT resources and systems at any time.

3.2 Acceptable Use of County IT Resources and Systems.**3.2.1 Lawful and Ethical Use.**

Use of County IT resources and systems shall not be fraudulent, unlawful, offensive, or disruptive. County IT resources and systems shall not be used to intentionally view, download, store, transmit, or retrieve any information, communication or material which is harassing or threatening; is obscene, pornographic or sexually explicit; is defamatory; makes discriminatory reference to sex, race, color, age, sexual orientation, religious or political beliefs, national origin, marital status, or disability; is untrue or fraudulent; is illegal or promotes illegal activities; is intended for personal profit; condones or fosters hate, bigotry, discrimination or prejudice; facilitates Internet gaming, gambling, bidding, or selling; or involves offensive content.

- 3.2.2 Legal Compliance.
Use of County IT resources and systems shall be in compliance with copyrights, licenses, contracts, intellectual property rights and laws associated with data, software programs, and other materials made available through those systems. Data and records maintained in these IT resources and systems shall comply with relevant federal and state access and privacy laws.
- 3.2.3 Confidentiality of IT Resources and Systems.
Users shall respect the confidentiality of County IT resources and systems and shall not attempt to: (i) access third party systems without prior authorization by the system owners; (ii) obtain or use other users' login names or passwords without their consent; (iii) attempt to defeat or breach computer or network security measures; (iv) intercept, access, monitor or peruse electronic files, information or communications without specific County business need to do so, and prior written approval from the responsible County agency management.
- 3.2.4 Data Integrity.
Users shall not knowingly destroy, misrepresent, or otherwise change the data or records stored in County IT resources and systems with the intent to conceal violations of laws, ordinances or policies.
- 3.2.5 Operational Efficiency.
Operation or use of County IT resources and systems shall be conducted in a manner that will not impair the availability, reliability or performance of County business processes and systems, or unduly contribute to system or network congestion.
- 3.2.6 Accounts and Account Passwords.
All users shall be properly authorized and authenticated to use County IT resources and systems.

3.3 **Personal Use of County IT Resources and Systems.**

Personal Use of County IT Resources and Systems.

Use of County IT resources and systems creates risk for the County. The County can only accept this risk for County business use.

County agency management may allow employees limited, incidental personal use as long as there is no significant risk or cost to the County and such use does not violate any County policy or impede the conduct of County business. County agency management, in consultation with County Information Services, shall have sole discretion on a case-by-case basis to determine if an employee's use is personal or business.

3.4 Specific Limitations on Personal Use

3.4.1 Internet Services.

County IT resources and systems shall not be directly connected to the Internet unless that connection is approved and provisioned by County Information Services.

3.4.2 County Network Services.

Personal, 3rd Party, or County IT resources and systems shall not be connected to the County network unless that connection is approved and provisioned by County Information Services.

3.4.3 Guest Internet Services.

Guest networks are provided at several County locations. Guest networks are provided for the convenience of the public and are to be considered "as-is" with no warranty of safety.

County IT resources and systems shall not be connected to any County provisioned "Guest" network or other network provided strictly for the convenience of the public.

3.4.4 Electronic Communication Services.

Electronic communication services, including e-mail messages, voice-mail messages, fax messages, or other electronic communications, which attempt to hide the identity of the user or represent the user as someone else is prohibited. Confidential information transmitted externally shall be appropriately protected.

Electronic communications may be a record under federal or state laws and regulations, and all users of County IT resources and systems are responsible for ensuring compliance with County policy regarding the archiving of government records.

Employees who terminate or are terminated have no right to their electronic communications and are not allowed to access any County electronic communication services. Employees who terminate are required to provide their supervisor with passwords or any other access information they may have to any electronic communication systems.

3.4.5 Personal Software, Content and Hardware.

Audio, video, and software files, which are personally owned and are for personal use, shall not be downloaded to, transferred to or installed on any County IT resource or system.

IT resources or systems, which are personally owned and are for personal use, shall not be connected or attached to any County IT resources or systems.

Subject to the limitations of Sections 3.2.1 of this policy, County agency management may allow users to play, but not download, transfer or install,

personal electronic audio or video media using County IT resources or systems provided County agency management determines it does not interfere with their or others' work, and provided that doing so does not access the County network.

- 34.6 Copyright Violations.
Any action that would result in copyright violation is prohibited. This includes but is not limited to copying of software applications, music files, videos, documents, files and other copyrighted materials.
- 34.7 Remote Access Systems.
Use of remote access systems that provide access to County IT resources or systems is allowed for County business use only. All remote access to County IT resources and systems must make use of County Information Service's approved and provisioned remote access systems.
- 34.8 Personal Use of Streaming Media Resources.
The County's Internet connection is a valuable, limited resource that is reserved for County business use only. Use of non-business related streaming media and video services is prohibited.
- 34.9 Personal Use of Encryption.
Personal hardware or software may not be used to encrypt information on any County IT resource or system.
- 34.10 Personal Solicitation.
County IT resources or systems shall not be used for personal solicitation, including solicitation for or against commercial ventures, products, religious or political causes, or outside organizations. Exceptions to this policy may be approved for causes or purposes supported by County agency management, which shall determine the exceptions on a case-by-case basis.
- 34.11 IM (Instant Messaging) or IRC (Internet Relay Chat).
The use of IM (Instant Messaging) systems or IRC (Internet Relay Chat) services for personal use is prohibited.
- 34.12 Proxy Avoidance and Anonymizer Services.
Any use of "Proxy Avoidance" or "Anonymizer" or "Anonymizing" services is prohibited.
- 34.13 Internet Communications Services.
Any use of Internet phone systems is prohibited.
- 34.14 Peer-to-Peer File Sharing.
Any use of P-to-P (Peer-to-Peer) file sharing networks is prohibited.

3.5 **Monitoring, Control, and Compliance**

Monitoring of County IT Resources and Systems

The County has the right, at its discretion, to monitor its IT resources and systems to ensure they are being used appropriately and are functioning properly. The County may monitor a user's individual use of IT resources or systems for any reason without notifying the user in advance.

County agency management is responsible for monitoring the use of County IT resources and systems, with the assistance of County Information Services (County IS). County IS will employ monitoring systems and processes to create usage reports. The resulting reports will be available for review by County agency management and County IS.

In the event County agency management suspects unacceptable activity, they shall contact Human Resources. If County IS suspects unacceptable activity, it shall consult with County agency management responsible for the user, after which County agency management will contact Human Resources if it suspects unacceptable activity.

Investigations into unacceptable activity shall be conducted by County IS and Human Resources, working together as a partnership, and not by any one of these individually.

3.6 **Training**

Information Security Awareness Training

All benefit eligible employees will be expected to participate in and complete appropriate information security awareness training on an annual basis. Information security awareness training will be provided by County Information Services in coordination with County agency management or their designee.

4.0 **Exceptions**

- 4.1 In limited situations employees may be required, as part of their assigned duties and responsibilities, to access the restricted information, referenced in 3.2.1 above, for legitimate County business purposes. In such cases, County agency management shall require and maintain written employee affirmation and County agency management approval of the exception, after which County IS will implement the technical requirements.
- 4.2 Those employees responsible for monitoring IT resources and systems or that are engaged in data investigations are permitted to do so as part of their assigned duties and responsibilities.
- 4.3 County agency management may allow greater than incidental personal use of County IT resources and systems if prior to such use County agency management approves this exception in writing and County IS determines in writing that the use does not pose an undue risk to County IT resources and systems.

County agency management may also allow the personally-owned items identified in Section 3.4.5 to be downloaded, transferred, installed or connected to County IT resources and systems if prior to such action, County agency management approves this exception in writing and County IS determines in writing that such action does not pose an undue risk to County IT resources and systems.

4.4 Additional exceptions to this policy shall be approved in conformance with County-wide 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.

6.0 Education

Training will be provided to County employees on this policy.

APPROVED and ADOPTED this 16 day of August, 2016.

SALT LAKE COUNTY COUNCIL

Max Burdick
Max Burdick, Chair

ATTEST:

Sherrie Swensen
Sherrie Swensen, County Clerk

APPROVED AS TO FORM:

D.W.K. Smith 7/21/16
District Attorney's Office Date