Utah County Human Resource Management Policy 2-2500: Information Technology Security and Acceptable Use Policy

Purpose

This policy is designed to ensure:

1. Information Technology (IT) resources and systems owned by Utah County are used efficiently and appropriately,
2. Utah County employees, volunteers, elected officials, and appointed officers are aware of the acceptable use of IT resources and systems, and
3. Utah County Information Systems Department will monitor the use of IT resources and systems and enforce compliance with this policy.

Objective

The objectives of this policy are to mitigate risk by:

1. Effectively managing security exposure or compromise of County IT resources and systems,
2. Communicating the responsibilities for the protection of County IT resources and systems and,
3. Promoting and increasing the awareness regarding information security.

I. Policy

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

B. Utah County is committed to implementing new technologies for communication and information storage, analysis, and exchange, when such will make the County's employees more productive and increase the County's capacity to better serve the residents of Utah County.

C. The County encourages the work-related use of information technology (IT) resources including computers and other electronic communication devices and services as effective and efficient communication tools and as valuable sources of information. Computers and other electronic communication devices and services provided by the County are County property, their purpose is to facilitate County business, and their use is subject to County control and policy.

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

II. Definitions

A. Active Directory (AD) Account
An Active Directory account allows Utah County employees, and employees of entities that contract with Utah County for IT services, to log into computers joined to the County's domain to access County IT resources and systems. Each employee has an individual Active Directory account assigned to them; it is an employee's personal identifying credential for access to County IT resources and systems.

B. Pornography
Any visual depiction, including any live performance, photograph, film, video, picture or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct.

C. Child Pornography
As defined in Utah State Code 76-5b-103, any visual depiction, including any live performance, photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. The production of the visual depiction involves the use of a minor engaging in sexually explicit conduct.

2. The visual depiction is of a minor engaging in sexually explicit conduct; or

3. The visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

D. Computer Technician
Information Systems staff, typically Computer Support Technicians, who in the course and scope of the individual's employment for compensation installs, maintains, troubleshoots, upgrades, or repairs computer hardware, software, personal computer networks, or peripheral equipment.

E. IT Resource(s) and/or System(s):
Computers, hardware, software, data, storage media, electronic communications (including, but not limited to, e-mail, fax), 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.

Utah County Human Resource Management Policy 2-2500: Information Technology Security and Acceptable Use Policy

F. Proxy Avoidance and Anonymizer Services
Services that are used to bypass content filtering safeguards and policies. Users of proxy avoidance and anonymizer services can connect to a proxy service in order to access websites that may otherwise be blocked by security controls.

III. Ownership, Access, and Expectation of Privacy

A. Ownership
County IT Resources and Systems are property of Utah County, not the user. No Utah 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, as determined by the Information Systems Department, regardless of which department purchased the resource or system. Employee e-mails, text messages, faxes, etc. generated on County IT resources or systems are County property and are subject to County monitoring, control, transfer or use despite any designation as confidential by the sender or recipient.

B. Access and Control
Utah County reserves and exercises all rights relating to all information and programming assets. The Utah County Information Systems Department is responsible for granting users' access to County 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. The Utah County Information Systems Department may withdraw permission for any or all use of its IT resources and systems at any time without notice.

C. Privacy
Employees have no reasonable expectation of privacy with their use of IT resources including but not limited to electronic communications sent to/from or stored on County IT resources or systems, and the 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. Users are subject to applicable public records retention laws and rules.

IV. Acceptable Use of County IT Resources and Systems

A. Lawful and Ethical Use
Use of County IT resources and systems shall not violate County Human Resources policies, including but not limited to "Harassment, Discrimination and Retaliation" and "Standards of Conduct." IT resources shall not be used for knowingly transmitting, receiving, retrieving, or storing any communications which are derogatory to any individual or group, are pornographic, lewd, indecent, or of a sexual nature, or are of a defamatory or threatening nature.

B. Legal Compliance
Use of County IT resources and systems shall comply 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.

C. Confidentiality of IT Resources and Systems

Users shall respect the confidentiality of County IT resources and systems and shall not attempt to:

1. Access third-party systems without prior authorization by the Information Systems Department;

2. Obtain or use another employee's login credentials to any County IT resources and systems;

3. Attempt to defeat or breach computer or network security measures.

4. Intercept, access, monitor or peruse electronic files, information, or communications.

5. Disseminate County data through unauthorized communication channels without specific County business need to do so,

6. Disseminate County programming code, or any proprietary or technological intellectual property of the County through unauthorized communication channels without specific County business need to do so, *and* prior written approval from the Information Systems Department.

D. Data Integrity

Users shall not knowingly destroy, misrepresent, or inappropriately change the data or records stored in County IT resources and systems.

E. 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 unnecessarily contribute to system or network congestion.

F. Accounts and Account Passwords

All users in the scope of this policy shall be properly authorized and authenticated to use County IT resources and systems. All those in the scope of this policy who use County IT resources and systems *shall never share their password with anyone for any reason*. Failure to protect your password may result in disciplinary action in accordance with County disciplinary policies.

Utah County Human Resource Management Policy 2-2500: Information Technology Security and Acceptable Use Policy

V. Personal Use of County IT Resources and Systems

A. IT resources and services provided for County business use and should not be used for personal, outside business or employment, or non-County related purposes. However, limited, occasional, or incidental use of electronic communication devices and services (sending or receiving) for personal, non-County purposes, is acceptable insofar as that use complies with County policy, does not interfere with the County's business activities, and so long as such use does not involve any use described under ***B. Specific Limitations on Personal Use*** section of this policy, or any of the following:

1. Interference with or violation of County rules or policies.

2. Disruption or distraction from the conduct of County business (e.g., due to volume or frequency)

3. A for-profit personal business activity

4. Potential to harm the County

5. Illegal activities

6. The display, storage or recording of any kind of sexually explicit, harassing, or discriminatory image or document. See Section IV.A.

B. Specific Limitations on Personal Use

1. **County Network Services**
   Personal, third-party, or County IT resources and systems shall not be connected to any County provisioned network unless that connection is approved by the Information System Department.

2. **Guest Internet Services**
   Guest networks access are provided at several County locations, typically through a Wi-Fi access point. Guest networks are provided for the convenience of the public and are to be considered "as-is" with no warranty of safety or security for the user. 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. **Electronic Communication Services**
   Electronic communication services, including e-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 from employment have no right to their electronic communications and are not allowed to access any County electronic communication services immediately upon termination.

4. **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 unless approved by the Utah County Information Systems Department and the employee's supervisor or department head.

5. **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 Information Systems Department approved and provisioned remote access systems. Telecommunicating users must comply with the Utah County Human Resource Management Policy 2- 1700: Telecommunicating.

6. **Personal Use of Streaming Media Resources.**
   The county's internet connection is a valuable, limited resource that is reserved primarily for county business use. Limited personal use of the county's internet connection is allowed, if approved by their department head, and only if it does not create a disruption of services to others. The Information Systems Department may, at its sole discretion and without warning, limit access to web services which are negatively impacting our ability to maintain effective operations.

7. **Personal Use of Encryption**
   Personal hardware, software, or encryption keys may not be used to encrypt information on any County IT resource or system.

8. **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.

9. **Proxy Avoidance and Anonymizer Services**
   Filtering of websites containing inappropriate or illegal content, suspected malware, phishing services, and other fraudulent services is an essential tool the County uses to protect the security of Utah County's IT infrastructure. Any use of "Proxy Avoidance" or "Anonymizer" or "Anonymizing" services to bypass this filtering is prohibited. See definition of Proxy Avoidance and Anonymizers in Section II.E.

Utah County Human Resource Management Policy 2-2500: Information Technology Security and Acceptable Use Policy

C. Monitoring, Control, and Compliance

1. 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 routinely monitors usage patterns and monitors and logs all internet usage for each county user.

2. No Expectation of Privacy

No county employee should have any expectation of privacy as to their IT resources usage including internet history and email. The County will review network activity, internet activity, and other IT resources and analyze usage patterns and may choose to disclose this data in any manner the County deems appropriate to assure that the County's IT infrastructure is being used appropriately and operating at the highest levels of productivity.

VI. Purchasing Third-Party Software, Programming, and Application Development, Web Domains

A. Procurement of Third-Party Software

Installation and use of third-party software has the potential to introduce dangerous security risks or impact negatively the performance of Utah County's IT infrastructure. All software purchases must have prior approval from the Information Systems Department.

B. Programming & Application Development

To mitigate security and performance risks to the County's IT infrastructure, all in-house programming should be reserved solely for Information Systems staff. All third-party contractors providing customized programming services or application development work must be vetted and approved by the Information Systems Department before contracts are signed. In addition, third-party contractor work must be coordinated by the Information Systems Department to ensure quality control and sufficient security is implemented.

C. Web Domains

Since a .gov domain is only available to bona fide US-based government organizations, using it signals trust and credibility. This establishes digital services (e.g. websites, emails) as official, trusted sources for information. All web domains managed and maintained by Utah County departments must be purchased and renewed by the Information Systems Department. All new web domains must end in a ".gov" suffix. Any non .gov (i.e., .com, .net, .org) should be migrated to a .gov domain as soon as possible.

VII. Reporting the Suspicious Activity, the Discovery of Inappropriate Content, Pornography, or Child Pornography on County IT Resources or Systems

A. Discovery of Suspicious Network Activity or Potential Phishing Emails

All users who discover suspicious network activity or receive electronic communication such as a phishing email should immediately notify the Information Systems Department by contacting the IT Operations Manager, the IT Operations help desk, or the IT Director.

B. Discovery of Inappropriate Content or Pornography by Users
All users who discover inappropriate content, including any form of pornography, harassing or discriminatory material on County IT Resources and/or Systems should immediately notify the IT Operations Manager, the IT Director or the Human Resource Department. The IS Department and Human Resources Department will coordinate as appropriate in response to any reported violation.

C. Discovery of Child Pornography by Information Systems Staff
A computer technician who in the course of employment for compensation views an image on a county computer, network hardware, or other electronic device that is, or appears to be, child pornography shall immediately report the finding, as required by law (section 76-10-1204.5, Utah Code Annotated 1953), to the IT Operations Manager or IT Director who shall report to County Human Resource and/or County Attorney for investigation and appropriate action. County Human Resources and/or County Attorney shall report the case to the local police department with jurisdiction or the Attorney General crime against children task force for appropriate criminal charges.

VIII. IT Security Awareness Program

Utah County takes its responsibility to protect County IT resources and systems seriously. To help County employees and those within the scope of this policy to understand the risks in using modern technology and how to effectively defend against cyber threats both at work and at home, County IT will provide various methods of training and testing on IT security awareness.

Mandatory Information Security Awareness Training
All County employees with an individual Active Directory account, and those within the scope of this policy, are required to complete IT security awareness training on an annual basis. The training, usually in the form of online modules or in-person presentations, is provided by Information Systems Department or a contractor approved by the Information Systems Department.

Employees are expected to participate in additional reinforcement training such as short videos, newsletters, webcasts, emails, surveys, and assessments as provided by Information Systems Department, or a cyber security contractor approved by the Information Systems Department.

IX. Education About Information Technology Security and Acceptable Use Policy

Training will be provided to County employees regarding this policy.

X. Enforcement

A. 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 Utah County network and can lead to other disciplinary action, up to and including dismissal from County employment.

B. Elected Officers. Any elected officer found to have violated this policy may be publicly censored and referred to the County Attorney or Utah State Attorney General by a member of the County Commission for further investigation and action.