

JORDAN RIVER COMMISSION

INFORMATION & COMMUNICATION TECHNOLOGY SECURITY POLICY

1.0 Background & Overview

The Jordan River Commission and its partner agencies use information and communication technology such as electronic hardware and software, digital services, and data and communication networks for employees' use in conducting Commission business.

The purpose of this policy is to establish basic rules for employee use of all work related technology services and networks, including the Internet, email, and digital storage and archives.

2.0 Information & Communication Technology Use Policies

The Internet can be misused in a variety of ways, including but not limited to:

- Downloading files that contain viruses, thereby endangering Commission and partner agency information services;
- Accessing objectionable material;
- Wasting work time by performing unauthorized research, or accessing non-business-related information and people, or for computer games or online games.

2.1 General Policies for Use of Information & Communication Technology, Including the Internet:

An employee does not have a right to privacy when using Commission information and communication technology or conducting Commission business, and employees should not expect or assume any privacy regarding the content of such data and communications. This includes the use of personal computers or electronic devices for Commission business. The Commission and its public agency partners reserve the express right to monitor and inspect the activities of an employee while accessing the information and communication technology at any time, and to read, use and disclose data and communications, such as email and messages. In addition, all software, files, information, and communications downloaded or sent via the Internet or other networks using Commission or partner resources are their respective records and property. Such records are subject to potential review and disclosure under the public disclosure law of the State of Utah. Even after a message has been "deleted," it may still be possible to retrieve it.

The Commission has the right to restrict or prohibit any employee from Internet or other network access for violation of the policy. Violations may also result in disciplinary action, up to and including termination.

Except as outlined here, use of information and communication technology of the Commission or its partner agencies are for Commission business only. Some limited personal use is permitted, so long as it does not result in expense to the Commission, does not interfere with the performance of duties, is brief in duration and frequency, does not distract from the conduct of Commission business and does not compromise the security or integrity of information or software of the Commission or its partner agencies. Such limited use shall not occur on "paid time," but is permitted immediately before or after work hours and during an employee's breaks. Some examples of allowable personal use include accessing a weather report or news item on the Internet, or transmitting an email or message to a family member to check on their safety.

Any Internet use, including limited personal use described above, must comply with applicable laws and Commission policies including but not limited to all federal and state laws, and Commission policies governing sexual harassment, discrimination, intellectual property protection, privacy, public disclosure, confidentiality, misuse of Commission resources, information and data security. All Internet use must be consistent with the Commission's Personnel Policies Manual.

The Commission's information and communication technology systems permit employees to perform jobs, share files, and communicate internally and externally with individuals and entities in the performance and conduct of Commission business. Employees are prohibited from gaining unauthorized access to another employee's email, message or other accounts, or sending email or messages using another employee's account or identity.

In order to prevent potential Commission liability, it is the responsibility of all Internet users to clearly communicate to the recipient when opinions expressed do not represent those of the Commission.

The Commission has the capability and reserves the right to access, review, copy, modify and delete any information transmitted through or stored in technology and communication information systems. The Commission may disclose all such information to any party it deems appropriate and in accordance with applicable law. Accordingly, employees should not use the Commission's information and communication technology systems to send, receive or store any information they wish to keep private. Employees should expect that anything sent, received or stored anywhere in the system will be available for review by any authorized representative of the Commission for any purpose, as well as the public as part of a public records request.

An employee should create and send only courteous, professional and businesslike messages that do not contain objectionable, offensive or discriminatory material. For example, it is prohibited to make jokes or comments which could offend someone on the basis of gender, race, age, religion, national origin, disability or sexual orientation.

Caution should be taken in transmitting confidential information on the computer system. Employees should use due care in addressing email messages to assure messages are not inadvertently sent to the wrong person inside or outside the Entity. Email creates a written record subject to court rules of discovery and may be used as evidence in claims or legal proceedings. Once sent, email cannot be retracted. Even after deletion at a workstation, email can be retrieved and read.

The safety, security and liability of the networks and resources of the Commission and its partners must be considered at all times when using information and communication technology. Any installed file, software or application shall be legally obtained and used, and when downloaded should be properly scanned for virus, malware or other digital risks. Employees are not to share or reveal passwords and other account credentials with any unauthorized individual.

While using the Internet, individuals may encounter information that is offensive or objectionable. Individual users must use their own judgement and capability to avoid such content, and be aware that the Commission has no control over broad information available on the Internet and is not responsible for such content.

Nothing in this policy prohibits the use and access of any information and communication technology system for bona fide law enforcement and investigation purposes.

2.2 Prohibited Uses of Information & Communication Technology:

The following is list of prohibited uses of Commission information and communication technology systems, which is not exhaustive but provides a general guide for unacceptable use:

- Personal Commercial Use – any personal use for conducting trade, business or sales transaction of goods or services
- Solicitation – the promotion through advertising or marketing for personal commercial use
- Copyright Violations – the unlawful reproduction or distribution of copyrighted material or information
- Discrimination / Harassment – sharing, distributing or sending messages or other content which is harassing, derogatory or discriminatory to employees, vendors, customers, or the public
- Political – political campaigning purposes, including supporting or endorsing candidates or ballot initiatives; this does not prohibit working with state and local political leaders on policy and legislative activity that is part of official Commission business, or personal political activity that does not violate any other Commission policy
- Aliases / Anonymous Messages – the use of aliases or transmission of anonymous messages for any purpose, except as provided in other Commission policies for legitimate reasons to report fraud or abuse
- Misrepresentation – the misrepresentation of an employee’s job title, job description, position or status with the Commission
- Social Networking – the accessing and/or creation of social networking sites, such as Facebook, Twitter, Instagram, Blogs and similar sites for purposes not related to Commission business
- Instant Messaging – messaging by text or through social media sites that is not related to official Commission business, except of limited personal use as outlined above
- Misinformation / Confidential Information – the release of untrue, distorted, or confidential information regarding the Commission and its partners or employees
- Non-Business Related and Inappropriate Information – the accessing, viewing, distribution, downloading, or any other method for retrieving non-Commission related information, including but not limited to gaming and entertainment sites, pornographic or sexually explicit sites, personal chat rooms, blogs and bulletin boards
- Unauthorized Access – unauthorized attempts to access any other person’s network or email, or personal financial accounts or information
- Sensitive / Proprietary Information – the display or transmission of sensitive or proprietary information of the Commission or its partners or employees to unauthorized individuals or organizations
- Spamming – sending large volumes of inappropriate or irrelevant email or messages from the Commission’s communication networks or resources

2.3 Individual Responsibilities:

Internet users are responsible for complying with this and all other Commission policies when using the resources of the Commission or its partner agency resources for accessing the Internet. Violation of this policy is grounds for disciplinary action, up to and including termination.