TRUCKEE TAHOE AIRPORT DISTRICT
POLICY INSTRUCTION

PI NUMBER: 502

Effective: May 22, 2019
Approved: May 22, 2019

SUBJECT: Network Use Policy

Overview

Computer information systems and networks are integral to business at Truckee Tahoe Airport District. The District makes substantial investments to acquire and maintain these systems which support business, capacity, and safety continuity.

Internet and Intranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, and network accounts providing e-mail and web browsing are the property of the District. These systems shall be used for business purposes in serving the operational demands and interests of the District.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information or information systems owned or operated by the District. It is the responsibility of every user to conduct their activities responsibly and to understand these guidelines and best practices.

1.0 Purpose and Scope

The purpose of this policy outlines the acceptable use of computer equipment and technologies owned or operated by Truckee Tahoe Airport District. *Acceptable use* is defined as activity related to a user's job in support of the District which conforms to this and other related policies. Inappropriate use risks virus attacks, loss of critical business data, compromise to network systems and services, and is subject to legal action.

This policy applies to all employed, elected or appointed network users, including all personnel affiliated with third parties, consultants, contractors, and all equipment owned or leased by the District.

2.0 Policy

a. Specific Information Security Practices

i. All terminals and workstations shall be logged off when not in use to prevent unauthorized access to sensitive information. Sleep settings are encouraged.

ii. Applications accessing District financial, personnel, or customer personal information shall be logged off when not in use.

iii. All users must have unique and strong (mixture of case, letters, number, special characters) passwords on their network access accounts. Users shall change passwords periodically.

iv. All PCs used for email or internet access shall have current security patches and anti-virus software. This is a managed service directed by the IT administrator.

b. General Use and Ownership

i. While the District desires to provide a reasonable level of personal privacy, users should be aware that data created on District systems as well as products made on behalf of the District on private resources remain the property of the District and subject to FOIA and all applicable public information requests.

ii. Employees are responsible for exercising good judgment regarding personal use. If there is any uncertainty, employees should consult their supervisor.

iii. For security and network maintenance purposes and to ensure compliance with this policy, authorized individuals of the District may monitor or audit equipment, systems and network traffic at any time.

c. Security and Proprietary Information

i. Information on District computer systems may be confidential. All data is subject to FOIA. Employees shall prevent unauthorized access to information and be aware all data is subject to public request, which shall be approved by management or District counsel.

ii. Encryption must be used when emailing or otherwise electronically transferring sensitive information.

iii. All systems used by employees that are connected to the District internet/intranet, whether owned by the employee or the District, shall have installed approved virus-scanning software with a current virus definitions.

iv. Employees must use extreme caution when opening e-mail attachments. Viruses or other malware are most often delivered via email. Any suspicious emails or email attachments should not be opened and shall be reported to the IT administrator.

d. Unacceptable Use

The following activities are, in general, prohibited. Employees may be specifically exempted from these restrictions during the course of their legitimate job responsibilities.

Under no circumstances is an employee or agent of the District authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing District-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

i. Prohibited System and Network Activities

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the District.
2. Unauthorized copying of copyrighted material including, but not limited to, the download and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the District or the end user does not have an active license is strictly prohibited. Clip-art, icons, or images readily available over the internet for presentation, without express copy right are exempt.
3. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Using a District computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
5. Making fraudulent offers of products, items, or services originating from any District user account.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port scanning, security scanning, or performing any type of network monitoring which will intercept data not intended for the employee's system, unless given explicit consent to do so.
8. Circumventing user authentication or security of any system, network or account.

9. Providing personal information about, or lists of District employees to other organizations.
10. Pornography or content deemed illegal or inappropriate.
11. Any content blocked by District web filtering.
12. Any activity while working on behalf of the District that interferes with productive work efforts including social media, gaming, shopping, and travel. Content that conforms to the District's social media policy is allowed.

ii. Prohibited Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or other "pyramid" schemes of any type.

e. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I understand and agree to follow the Network Use Policy of Truckee Tahoe Airport District.

Signature_____ Date_____

Name_____