CENTRAL OREGON INTERGOVERNMENTAL COUNCIL

NETWORK AND DEVICE ACCEPTABLE USAGE COMPUTER POLICY

Date: April 1, 2017 (revision)

STATEMENT OF POLICY

1. COIC recognizes that use of the Internet/Intranet and e-mail has many benefits and can make workplace communication more efficient and effective. All employees, including any volunteers and interns are encouraged to use the Internet/Intranet and e-mail systems appropriately. This policy outlines COIC's guidelines for acceptable use of the Internet/Intranet and e-mail. A primary objective is to ensure the security and reliability of COIC equipment, information, and network. Unacceptable use of the COIC equipment, network or COIC data may lead to disciplinary action. Employees using COIC equipment and communication systems have no reasonable expectation of privacy in these systems, or any information found on these systems.

APPLICABILITY

This Policy applies to all COIC employees, volunteers, and interns (herein "Staff") who use COIC computers, electronic data equipment and communication networks.

Basic Rule

When performing any task on your computer, it is your responsibility to ensure your activities do not negatively impact the computer and network hardware at COIC. When in doubt about the possible consequences of your activities, consult IT. Be aware that there are many programs that COIC administers, and that COIC's network is relied on and utilized by all of them.

Guidelines

The following guidelines established for Staff use of the COIC's technology and communications networks, including the Internet/Intranet and e-mail, in an appropriate, ethical and professional manner.

2. All technology provided by COIC, including computer systems, electronic data equipment, communications networks, records and other information stored electronically, is the property of COIC and not Staff. In general, use of COIC's technology systems and electronic communications should be job-related and not for personal convenience, however COIC recognizes that employees may occasionally and for limited purposes use email or the internet for personal use. This recognition is not permission to use email or internet beyond limited and minimal purposes. Such limited use should only be during breaks and lunch periods. Employees abusing this privilege may be subject to disciplinary sanction.
3. Staff may not use COIC's Internet/Intranet, e-mail or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference or of a similarly related discriminatory or inflammatory nature may be transmitted. Harassment of any kind is prohibited.
4. Disparaging, abusive, profane or offensive language; materials that might adversely or negatively reflect on COIC or be contrary to its legitimate business interests; and any illegal activities, including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet/Intranet or e-mail, are forbidden.

5. Copyrighted materials belonging to entities other than COIC may not be transmitted by Staff on the network without permission of the copyright holder. Staff must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy for reference only. Saving copyright-protected information to a network drive without permission is prohibited. Sharing the URL (uniform resource locator or "address") of an Internet site with other interested persons for business reasons is permitted.
6. Staff may not use the system in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and "spamming" (sending e-mail to thousands of users.)
7. To prevent contamination of COIC technology and communications equipment and systems by harmful computer viruses, downloaded files should be checked for possible infection through the IT Department ("IT"). Also, given that many browser add-on packages (called "plug-ins") may not be compatible with other programs and may cause problems for the systems, downloading plug-ins is prohibited without prior permission from IT.
8. All COIC Staff is responsible for the content of all text, audio or image files that he or she places or sends over the Internet/Intranet and e-mail systems. No e-mail or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. COIC's organizational identity is attached to all outgoing e-mail communications, which should reflect its values and appropriate workplace language and conduct. Email signature will include an employees name, job position and COIC contact information and will not include personalized "tag" lines or quotes, logos not related to COIC or similar messages,
9. E-mail and other electronic communications transmitted by COIC equipment, systems and networks are not private or confidential, and they are the property of the company. Therefore, COIC reserves the right to examine, monitor and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite. Employees using COIC equipment and communication systems have no reasonable expectation of privacy in these systems, or any information found on these systems.
10. Internal and external e-mail, voice mail, and text messages are considered part of COIC's communication network. They are business records and may be subject to discovery in the event of litigation. Staff must be aware of this possibility when communicating electronically within and outside COIC.

Hardware

COIC's managed computerized-devices (such as workstations, laptops, printers, monitors, etc.) may only be installed, disconnected, moved, or removed only with permission from IT.

All network service-providing devices such as servers, routers, switches, and other related hardware contributing to or responsible for networking operations on COIC's network; and hardware that affects COIC's program-wide operations, may only be installed, moved, modified, disconnected, removed, or serviced by IT.

COIC contractors (i.e. BendTel and Bend Broadband), with the express knowledge of IT, and only within their scope of work, may move, modify, disconnect, or service COIC's network service-providing devices.

COIC IT equipment may only be moved to a different building or site after notifying COIC's Executive Assistant.

Desktop Computers, Laptops, and devices that exceed $499.99 in value must have a COIC asset tag.

Intentional destruction or tampering of any COIC equipment or networks by unauthorized Staff is strictly prohibited.

Devices, software, or hardware (such as screen sharing applications, personal smart phones, USB flash drives, etc.) not owned or managed by COIC are prohibited from access to COIC's network without express permission of IT.

Designated public Wi-Fi access points are exempt from this rule, but must be restricted from access to COIC's internal network, and verified by IT Staff.

Hardware of any kind connected for the purpose of enhancing, analyzing, diagnosing, or monitoring COIC traffic may only be connected to COIC's network with the expressed consent of IT.

Hardware of any kind connected for the purpose of infiltrating, hindering, sabotaging, or reducing the performance of hardware, software, or assets of COIC and non-COIC property is strictly prohibited.

Software

IT must be informed of all software installed on any computerized devices, regardless of location or device purpose, and is subject to the scrutiny of IT and managers for the program to which the equipment belongs.

Software which is found to have an adverse effect on COIC's network performance, contain malware or viruses, or poses a security risk to COIC, or suspect as such, may be removed and banned from use by staff at the discretion of the IT.

Authorized software installed on COIC computerized devices for the purposes of monitoring the device for viruses, malware, or security purposes, must not be removed or tampered with without the express knowledge and consent of IT.

Software installed on COIC hardware having the intended or unintended purpose of infiltrating, hindering, sabotaging, intentionally reducing the performance of, or intruding on COIC or non-COIC hardware or software is prohibited from installation or use on COIC devices of any kind.

Software installed on COIC hardware having the intended or unintended purpose of monitoring, recording, intercepting, analyzing, decrypting, blocking, or modifying network communication between devices on COIC's network or WAN connections is prohibited from installation or use without the express consent of IT, and only with a clearly defined scope of intent.

IT Managed Areas

Rooms designated for the storage and operation of COIC-managed network hardware, servers, computers, phone systems, and other technologies (aka Server Room) may only be entered by COIC IT or managers for the program that the equipment resides.

Server rooms must remain locked at all times unless under constant supervision by designated, staff and a purpose exist within reason for keeping the area unlocked.

Server rooms are prohibited from access by non-COIC staff without expressed consent of IT, with the following exceptions:

- A COIC contractor, with a clearly defined scope of work, and with the express knowledge of IT, may enter server rooms within that scope.
- If a co-occupancy agreement exists with other agencies, the server room is within the realm of that agreement, and the person is an authorized staff member of that agency or acting within the bounds of the co-occupancy agreement.
- The person is accompanied by IT, and has a reasonable purpose for being there.

Duty to Act

COIC employees who witness suspected violations of this policy should notify their immediate manager. Managers must report these incidents to IT as soon as possible.

Do not attempt to remove or remedy potential viral, malware, or other infections on your own. If you believe your computer is infected, power it off and contact IT immediately.

Additional Policies

In addition to the policies defined in this document, additional policies may exist based on the constraints of the program in which COIC staff resides. Some of these include HIPAA, FERPA, PCI, or regulations that influence policies for your program. Please consult with your manager or program administrator for details regarding these additional policies if applicable.

Software:

Employees must receive approval from IT prior to any installation including the downloading of software onto any COIC equipment. To prevent computer viruses from being transmitted throughout COIC's e-mail and Internet/Intranet system, there will be no downloading of any unauthorized software. All software downloaded must be registered to COIC.

Computer Systems:

All electronic data storage networks and computer systems and information stored therein are the property of COIC. No part of the system or the information provided therein is considered the private property of the specific user and there is no reasonable expectation of privacy. COIC retains all legal rights to control, transfer, or use all or any part of the system.

Copyright Issues:

Staff using the Internet/Intranet and e-mail system may not transmit copyrighted materials belonging to entities other than COIC. Please note that non-adherence to this policy puts COIC in serious legal jeopardy and opens COIC up to significant lawsuits and public embarrassment. All Staff obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission.

Security:

COIC may routinely monitor usage patterns in its Internet/Intranet and e-mail communications. The reasons for this monitoring are many, including cost analysis, security, bandwidth allocation and the general management of COIC's gateway to the Internet/Intranet. All messages created, sent or retrieved over COIC's e-mail and Internet/Intranet is the property of COIC and should be considered public information. COIC reserves the right to access and monitor the content of all messages and files on COIC's e-mail and Internet/Intranet system at any time with or without notice. Employees should not assume electronic communications are totally private and should transmit highly confidential data in other ways.

Violations:

Any employee who abuses the privilege of COIC's facilitated access to e-mail or the Internet/Intranet or who violate the terms and intent of this policy may be subject to disciplinary action up to and including termination. Disciplinary Procedures are defined in the COIC Personnel Policy, Section 21.0. If necessary, COIC also reserves the right to advise appropriate legal officials of any illegal violations.

Inquiries:

Inquiries should be addressed to the IT Manager at (541)548-9532.

Karen Friend

Executive Director