Policy No. 2016-01
February 18, 2016

MISSOULA COUNTY
ACCEPTABLE USE OF TECHNOLOGY POLICY

Purpose
The purpose of this policy is to outline the acceptable use of technology at Missoula County (the "County). The provisions of the policy have been established to protect the County and its employees from risks arising from the use of technology such as virus attacks, compromises of network systems and services, and loss or corruption of data.

Scope
This policy is applicable to all County departments and entities. For purposes of this policy, "employee" includes elected officials, appointed members of County boards, commissions, and councils, and all other temporary or permanent employees.

This policy applies to electronic and computing devices, software, and network resources used to conduct Missoula County business or interact with internal networks and business systems.

Administration
The Missoula County Director of Technology is responsible for administering, interpreting, and applying the terms of this policy. Department heads are responsible for the implementation of the policy within their departments and ensuring employee compliance.

Public Information
Most employee communications and documents are public documents under Montana law and it is important that employees conduct themselves in a manner consistent with their public duties. Employees should not expect any right to privacy of documents and communications created in the course and scope of their employment. While most communications and documents are subject to public disclosure, some documents and communications are considered confidential or private by law. Employees must follow county policies for the protection and release of any information to avoid disclosure of information that is not public information.

References
Missoula County Technology Acquisition Policy, Communications Policy

Policy

<u>Introduction</u>

Technology, including but not limited to, internet/intranet/extranet-related systems, computer equipment, software, operating systems, storage media, network accounts,

electronic mail, web browsing, and file transfer protocol is provided to employees to serve the interests of Missoula County and its residents. Such technology is the property of Missoula County and is subject to security measures designed to protect the underlying systems and prevent interruptions in service.

Effective security is a team effort involving the participation and support of every Missoula County employee who deals with information and/or information systems. All computer users should be familiar with system security and the acceptable uses of technology and conduct their activities accordingly.

General Use and Ownership

1. Missoula County is the sole owner of County information stored on electronic and computing devices, whether owned or leased by the County, an employee, or a third party.
2. As soon as any theft, loss, or unauthorized disclosure of Missoula County information is detected, it should be reported to Missoula County IS Helpdesk.
3. County information should be accessed only to the extent that it has been authorized and is necessary to fulfill an employee's job duties or to satisfy public information requests.
4. Good judgment should be exercised when using County technology for personal purposes. Excessive use of these systems for personal matters is prohibited.
5. For security and network maintenance purposes, authorized individuals within the County may monitor equipment, systems and network traffic at any time.
6. Missoula County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. System level and user level passwords must comply with Missoula County's current password protocols. Providing a password or allowing account access to another, either deliberately or through failure to secure its access, is prohibited.
2. All computing devices must be secured with a password-protected screensaver with an automatic activation feature set to 20 minutes or less, unless the Technology Department authorizes an exception.
3. Logging off or locking is required when a device is left unattended.
4. Caution must be used when opening e-mail attachments received from unknown senders, as such attachments may contain malware.
5. All Missoula County Technology users will be required to take a cyber security awareness course administered by the Technology Department on a yearly basis. Alternative courses may be approved.

Unacceptable Use

County employees are prohibited from using County-owned resources to engage in any activity illegal under local, state, or federal law.

An employee’s use of County systems indicates recognition of the County's right to monitor use of these systems.

The following activities are, in general, prohibited. This list is not exhaustive but attempts to provide a framework for categories of use considered unacceptable.

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, the installation of software products not appropriately licensed for use by the County;
2. Unauthorized reproduction of copyrighted material including, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the County does not have an active license;
3. Offering for sale illegal substances or activities or making fraudulent offers of products, items, or services;
4. Accessing data, a server, or an account for any purpose other than conducting County business, even if access is authorized;
5. Introducing malicious programs into the County network or servers (eg, viruses, worms, Trojan horses, email bombs, etc);
6. Downloading or transmitting information or messages that may reasonably be considered offensive, pornographic, discriminatory, defamatory, disparaging, or threatening to any employee, person or entity;
7. Making statements about warranty, expressly or implied, unless part of normal job responsibilities;
8. Effecting security breaches or disruptions of network communication;
9. Port or security scanning without authorization from the Technology Department;
10. Executing any form of network monitoring designed to intercept data not intended for the employee's computer;
11. Circumventing user authentication or security of any host, network or account;
12. Introducing honeypots, honeynets, or similar technology on the County network without approval by the Technology Department;
13. Interfering with or denying service to any other user
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/intranet/extranet.

Email and Communication Activities

The following activities are prohibited:

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. Failure to respect the conventions, courtesies, and rules governing electronic communications;
3. Forging email header information;

4. Soliciting email for another 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", "Ponzi" or other "pyramid" schemes of any type;
6. Posting the same or similar non-business related messages to large numbers of usenet newsgroups (newsgroup spam);
7. Using County systems for outside business ventures, to leak confidential or privileged information, or for political or religious causes; and
8. Excessive use of these systems for personal matters.

Policy Compliance
The Technology Department will verify compliance with this policy. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Human Resources will be consulted prior to all disciplinary action.

The Technology Department must approve in advance any exception to this policy.

Definitions and Terms
The following definitions and terms may be found in the SANS glossary located at https://www.sans.org/security-resources/glossary-of-terms/:

file transfer protocol
honeypot
host
internet
intranet
malware
spam
Trojan horse
virus
worm
www

Wikipedia may be used to find definitions for: https://en.wikipedia.org/wiki/Main_Page

email bomb
extranet
honeynet
usenet