# SECTION 5.12
# EMAIL ACCESS AND SECURITY

## Overview

E-mail at **Jefferson County** must be managed as valuable and mission critical resource. Thus, this policy is established to:

- Create prudent and acceptable practices regarding the use of information resources
- Educate individuals who may use information resources with respect to their responsibilities associated with such use
- Educate individuals on the proper security practices that are required to maintain a safe and working email infrastructure.

## Purpose

The purpose of this policy is to establish rules for the use of **Jefferson County** email, for sending, receiving, or storing of electronic mail.

## Scope

This policy applies equally to all individuals granted access privileges to any **Jefferson County** information resource with the capacity to send, receive, or store electronic mail.

## Legal

Individuals involved **may** be held liable for:

- Sending or forwarding e-mails with any libelous, defamatory, offensive, racist, or obscene remarks
- Sending or forwarding confidential information without permission
- Sending or forwarding copyrighted material without permission
- Knowingly sending or forwarding an attachment that contains a virus
- Knowingly by-passing security measures for the purpose of inflicting damage to Jefferson County's systems and/or reputation

## Policy

All e-mails, files, and documents – including personal e-mails, files, and documents, that are not subject to other regulations such as HIPAA or client attorney privilege – are owned by Jefferson County, may be subject to open records requests, and may be accessed and/or audited to maintain security in accordance with this policy.

Incoming email must be treated with the utmost care due to the inherent information security risks. An anti-virus application is used to identify malicious code(s) or files. All email is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Spam will be quarantined for the user to review for relevancy. Introducing a virus or malicious code to Jefferson County systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, MIS must be immediately notified.

Anti-spoofing practices have been initiated for detecting spoofed emails. Employees should be diligent in identifying a spoofed email. If email spoofing has occurred, MIS must be immediately notified.

Incoming emails are scanned for malicious file attachments. If an attachment is identified as having an extension known to be associated with malware, or prone to abuse by malware or bad actors or otherwise poses heightened risk, the attachment will be removed from the email prior to delivery. Email rejection is achieved through listing domains and IP addresses associated with malicious actors. Any incoming email originating from a known malicious actor will not be delivered. Any email account misbehaving by sending out spam will be shut down. A review of the account will be performed to determine the cause of the actions.

E-mail is to be used for county business purposes and in a manner that is consistent with other forms of professional business communication. All outgoing attachments are automatically scanned for virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm Jefferson County's reputation. The following activities are prohibited by policy:

- Sending e-mail that includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, or threats to personhood outside of the county
- Using county e-mail for conducting a personal business.
- Using e-mail for the purposes of sending SPAM or other unauthorized solicitations.
- Violating copyright laws by illegally distributing protected works.
- Sending e-mail using another person's e-mail account, **except when authorized to send messages for another while serving in an administrative support role**.
- Creating a false identity to bypass policy.
- Forging or attempting to forge e-mail messages.
- Using unauthorized e-mail software.
- Knowingly disabling the automatic scanning of attachments on any Jefferson County personal computer.
- Knowingly circumventing e-mail security measures.
- Sending or forwarding chain letters, or hoax letters.
- Sending unsolicited messages to large groups, except as required to conduct Jefferson County business.
- Sending excessively large messages or attachments.
- Knowingly sending or forwarding email with computer viruses.
- Setting up or responding on behalf of Jefferson County without proper authorization.

All confidential or sensitive Jefferson County material transmitted via e-mail, outside Jefferson County's network, must be encrypted. Passwords to decrypt the data should not be sent via email.

**E-mail is not secure**. All user activity on Jefferson County information system assets is subject to logging and review. Jefferson County has software and systems in place to monitor email usage.

E-mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Jefferson County, unless appropriately authorized (explicitly or implicitly) to do so.

Users must not send, forward, or receive confidential or sensitive Jefferson County information through non-Jefferson County email accounts. Examples of non-Jefferson County e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and e- mail provided by other Internet Service Providers (ISP). Users with non-Jefferson County issued mobile

devices must adhere to the Personal Device Acceptable Use and Security Policy for sending, forwarding, receiving, or storing confidential or sensitive Jefferson County information.

## Access and Security

Email access is defined by either:

a. Going to a web browser and logging directly into a web portal to access the account.
a. Using any mail features or tools built in to the browser or web app to open employee accounts assigned to an individual.
c. Configuring any app that is installed locally on the machine to access to an email account.

Email access does not refer to any of the Administrator options or tools provided by Microsoft available to those who are providing administration, maintenance or security to the accounts.

All email access for Jefferson County will be secured with Multi Factor Authentication (MFA). Burden of Proof is on the User; the person making the claim, who they are, while attempting to access the email account. The user must provide a security token transmitted by the Authenticator, or a 6-digit code texted to them.

It is the responsibility of the Users to maintain any and all forms of Multi Factor Authentication needed to access email. If a provisioned authentication method is lost or damaged it is the user's responsibility to inform MIS to have another method setup.

MFA is essential to maintaining a secure email infrastructure and preventing unauthorized email access. This also allows MIS to be transparent as we cannot turn on or off MFA without a log being created that can be audited. If MFA needs to be turned off, MIS will notify users of the actions to inform user of a reduced security state of the account. Although System administrators within MIS are able to access email accounts without express consent of end users, we will not unless:

- Legal action requires MIS to retrieve email or logs
- The user is available but refuses to act on legal action brought before Jefferson County to access email.
- There is an alert of potential security incident.
- There is a request to MIS to do administration on an account (ie. Supervisor wants multiple people to have access to a mail box or a request to investigate emails).
- The user is not an employee of Jefferson County anymore.
- Maintenance is needed to maintain the integrity of the email system.
- Vender Changes that effect the county and the email services that they provide.

## Personal and Unauthorized Use

Personal use of sending e-mail is restricted to Jefferson County approved users, MIS will defer to departmental approval. Use of the account does not extend to family members or other acquaintances and is considered unauthorized. Without prior management approval, personal use must not result in direct costs to Jefferson County. Personal use must not interfere with the normal performance of an employee's work duties.

No files or documents may be sent or received that may cause legal liability for or embarrassment to Jefferson County. Storage of personal files and documents within Jefferson County's computer systems should be nominal.

## E-mail Retention and Size restrictions

Email retention will be based on license type, size of mailbox and/or archive. The types of licenses used are Frontline Worker license and Supervisor/Elected official license.

*Frontline Worker License**

- If this tier of license is provided to the user, they will have a mailbox size of 2GB. Any mail that exceeds that capacity will be subject to be purged, starting with the oldest mail first.
- Emails older than 36 months are subject to automatic purging.
- The archive folder this tier of license is part of the 2GB mailbox size.
- Deleted and archived emails are subject to automatic purging.
- Appointments, Tasks, and Notes older than the retention period are subject to automatic purging.
- Any email that you feel you need to keep longer than the retention policy you must save or print out.

*Supervisor/Elected Official License**

- If this tier license is provided to the user, they will have a mailbox size of 50GB and a separate archive folder of 100GB.
- It is up to the user to archive email if they so wish.
- There will be no time restriction on the mailboxes just a size restriction. If the size exceeds the given capacity emails will be subject of being purged, starting with the oldest mail first.

*Although there are no retention dates for this tier of license it is still recommended that you only keep email for only a given time. All email is subject to open records requests.*

*All Licenses are subject to change according to the public availability and financial obligations of Jefferson County.