Title: Administrative Policy Use of Information Technology Resources	**Policy No.** Part 5, Staff Policies Chapter 4, Information Technology Security and Safety Section 1
	Effective Date January 1, 2020
Policy Custodian Business Innovation and Technology Division	**Adoption/Revision Date** December 17, 2019

Adopting Resolution(s): CC19-427

References (Statutes/Resos/Policies): CC07-467, CC10-473, CC14-204, CC16-010, CC19-283, CC19-283; Information Security Advisory Committee Policy; Cyber Security Training Procedure

Purpose: To ensure the proper use of the Jefferson County Information Technology Resources and establish roles and responsibilities to ensure the completion of cyber security training necessary for protecting against and responding to issues that could be related to cyber threats against county information technology resources.

A. Definitions

1. Cyber Security Training: Training to provide every employee a fundamental understanding of the imminent and ongoing cyber threats that can lead to incidents and breaches of the county's information technology resources. Cyber security training prepares employees to identify and protect the organization from common cyber-attacks and cyber threats.

2. Cyber Attack: Any one or more of the following:
   - Phishing. Phishing is a common practice used to target a large number of users with emails that look genuine but are actually intended to lead untrained users to click on dangerous links, open unsafe attachments, or provide confidential or personal information.
   - Spear phishing. Spear phishing takes a targeted approach to attack specific individuals and organizations. The email is often hand-crafted and uses available information to make the email read exactly like an actual email from a known associate.
   - Malware. Short for "malicious software", malware refers to any type of software designed to interfere with a computer's normal functioning.
   - Ransomware. Malware that requires the victim to pay a ransom to access encrypted files. Ransomware is used by attackers to extort money (or possibly other resources) from the target organization.
   - Social engineering. The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

B. Applicability

1. This Policy shall apply to all Elected and Appointed Officials and all employees, volunteers, and contractors.

2. Covered employees and other individuals.

3. Some County Departments/Offices may impose procedures, standards and processes beyond those outlines in this policy. Employees may be required to confirm that they have read, understand and agree to abide by this policy as well as any applicable procedures and/or standards.

C. Roles and Responsibilities

1. Department/Division Directors and Elected/Appointed Officials shall be responsible for the following:
   - Ensuring their employees are aware of and promote the need to complete IT Resource training, including cyber security training, and review any applicable policies, procedures, standards or guidelines to protect the county's Information Technology Resources.
   - Requesting additional training through their technical support staff if the standard training is not sufficient to protect county Information Technology Resources.

2. Chief Information Security Officer shall be responsible for collaborating with the Information Security Advisory Committee to oversee IT Resource training tools, tests, reports, the standard content to be delivered, and supplemental training.

3. All staff with access to electronic resources shall be responsible for the following:
   - Completing assigned IT Resource training, including cyber security training, unless the employee or staff member is on leave or not working.
   - Understanding and complying with the material presented in the trainings.
   - Reporting potential cyber attacks immediately to their technical support staff.
   - Reviewing and acknowledging all county policies that are assigned as part of the IT Resource training.

D. Acceptable Usage

1. Jefferson County provides a variety of Information Technology (IT) Resources including, but not limited to, smartphones, computers, Internet, Email, Telephone, FAX, Video and specialized applications that are used to conduct business of the county. Use of these services must be consistent with conventional standards of ethical behavior and professional conduct and must not be knowingly used to violate the laws and regulations of the United States, or any state, city, county, or other local jurisdiction in any way. Use of any IT Resource for on-line gaming, gambling, and viewing of harassing, or pornographic sites is prohibited unless required by the employee's work assignment(s).

2. The Business, Innovation and Technology (BIT) Division may create and maintain procedures, standards, and other documents that provide additional examples regarding the acceptable use of county IT resources. Some Departments/Offices may impose additional procedures, standards and other documents. Employees should check with their management to determine if any apply. Employees may be required to confirm that they have read, understand and agree to abide by this Policy, and any applicable procedures, standards, and/or other documents.

3. The county reserves the right to review usage logs, files, emails, and other records at any time in accordance with applicable confidentiality laws. Employees have no right of privacy when using any county device or service and should hold no such expectation. Usage logs may be subject to open records requests.

4. Employees may use county IT resources for personal use when use does not interfere with the performance of the employee's duties as determined by the employee's supervisor, does not interfere with the performance of county IT resources, does not negatively impact or conflict with security requirements of county maintained information, and does not cause an additional cost to the county, such as charges for long distance calls and text messaging.

5. Failure to comply with this Policy may result in loss of privileges and disciplinary action as provided for in the Personnel Rules.

E. Security

1. All devices connected to the county information technology networks or containing sensitive or confidential information shall be secured in the manner identified by BIT or appropriate IT unit within a Department/Office that best protects the network and/or information.

2. Employees shall not disclose or share computer system logins and passwords or authorize others to use their passwords and account information for any purpose unless approved by the IT unit within a Department/Office.

F. Electronic mail

Email shall not be used to create, forward, or display any offensive or disruptive messages or to solicit or lobby others for commercial, religious, political or other similar ventures unrelated to county business. Jefferson County email addresses may not be used in non-business-related forums.

G. Software

1. Employees shall not transfer to any third party any software owned or licensed by the county without explicit written authorization from BIT, the County Attorney's Office, and the appropriate Department/Division Director or

Elected/Appointed Official responsible for the software. All such transfers shall be consistent with any applicable license terms and restrictions and transferred in a manner so as to protect the security of the county's data and proprietary software.

H. Any software installed or downloaded to county-owned computers must be approved by BIT or appropriate IT unit within a Department/Office.

1. Employees shall be responsible for the appropriate use and protection of county data and information.

2. Employees shall not willfully access or look at confidential or sensitive information without authorization except when necessary to conduct job duties.

3. Employees shall not transfer to any third party any confidential information or data without explicit written authorization from BIT, the County Attorney's Office, and the appropriate Department/Division Director or Elected/Appointed Official responsible for the information and data unless required or permitted by the terms of a contract that has been reviewed and approved by the County Attorney's Office. All such transfers shall be consistent with any applicable third party restrictions for non-county information and data and in a manner so as to protect the confidentiality of county confidential information and data.

4. These requirements apply to paper and other physical forms of documents and information and to voice and digital information contained in all electronic systems owned or used for county business.

I. Internet
Only those employees or Officials whose job duty it is to speak or write on behalf of the county may speak or write in the name of the county on the Internet. The Internet is a public forum where it is inappropriate to reveal confidential information and any other material whose distribution is restricted by county policies or procedures.

J. Cell Phones and Smart Phones

1. Elected Officials, Appointed Officials and Department/Division Directors shall determine which employees will be issued a county cell phone or smartphone.

2. The employee's Elected Official, Appointed Official or Department/Division Director may authorize use of employee owned cell phones and smart phones. Elected Officials, Appointed Officials and Department/Division Directors may approve appropriate employee reimbursement for business use of such employee owned devices.

3. If a telecommunication device, county or employee owned, used to connect to

the county's phone or data network is lost, stolen, or damaged, the employee must immediately notify his/her supervisor and his/her IT service support desk. Employees may be responsible for the replacement cost of county owned devices and are responsible for the replacement of employee owned devices.

4. Telecommunications devices may be used for personal purposes if the county will not incur an additional charge, such as for long distance calls. Accidental charges shall be reported immediately to the Elected Official, Appointed Official or Department/Division Director to determine acceptability and accountability. If unsure whether a particular charge is within the bounds of this Policy, the employee shall contact his/her IT service support desk for clarification.

5. Employees must pay for non-business-related cell phone and smart phone applications. All business-related applications may be downloaded upon approval of the employee's supervisor. Business related applications may be paid for by the county at the discretion of the employee's Elected Official, Appointed Official or Department/Division Director.

K. Home Use of IT Equipment
County-owned IT equipment (PCs, printers, etc.) and associated supplies may be taken home by employees for use in the performance of their job upon approval of the employee's supervisor. All equipment must be returned upon separation of employment with the county.

L. Cyber Security Standards

1. Training
   - Cyber security training shall be delivered to all staff. Additional training will be delivered to employees in high-risk positions (including but not limited to those with access to sensitive data, compliance data, and those with the ability to perform financial transactions).
   - Additional training shall be delivered to all technology support staff ensuring they can also function as experts when staff and employees contact them with questions.

2. Testing
   Simulated cyber-attack exercises will be done periodically.

3. Reporting
   - Regular reports to managers and division/department heads or their designated representative will be made available.