Title: Administrative Policy Information Technology Resources	**Policy No.** Part 5, Staff Policies Chapter 4, Information Technology Security and Safety Section 4
	Effective Date June 9, 2020
Policy Custodian Business Innovation & Technology	**Adoption/Revision Date** June 9, 2020

Adopting Resolution(s): CC20-133

References (Statutes/Resos/Policies): CC91-390, CC02-602, CC04-626, CC07-467, CC16-478

Purpose: To ensure compatibility, access, and protection of Jefferson County's Information Technology and Electronic Information.

Procedure: Yes

Policy: Information Technology Resources

A. Definitions

1. Information Technology Resources

   a. Hardware and Equipment: Includes all physical devices that are capable of accessing, storing, transmitting or processing Electronic Information. This includes, but is not limited to, network devices, servers, workstations, printers/copiers, fax machines, laptops, tablets, smartphones, USB memory devices and CD/DVD. Hardware used to store, transmit or process electronic information solely on state or federal networks are excluded.

   b. Software: Executable code that operates on Hardware.

   c. Internet Services: Services provided that are used for transmitting, accessing, storing or processing County Electronic Information. This includes, but is not limited to Internet Service Providers (ISP), email, on-line computing/storage, and on-line applications whether by purchase, subscription or for free.

   d. Mobile Devices: Any devices that are capable of being used to store, transmit or process Electronic data.

   e. Electronic Information: Information that is stored or transmitted in clear or encrypted formats on Hardware or Internet Services.

B. Responsibilities of the Chief Information Officer or designee

1. The Board of County Commissioners (BCC) designates the Director of the Business Innovation & Technology Department as the Chief Information Officer (CIO) for Jefferson County. In the event there is a vacancy in the position, the BCC authorizes the County Manager, to designate and name an employee to serve as the CIO.

2. Responsibilities of the CIO include:

    a. Coordinate distribution of this policy and any applicable procedures, standards, and/or other documents, to county elected or appointed officials, employees, volunteers, contractors, business partners and vendors that utilize County Information Technology Resources to store, transmit or process Electronic Information.

    b. Oversee an annual review and update of this policy and any applicable procedures, standards, and/or other documents needed to reflect changes to business objectives. Review proposed amendments to any policies or procedures that may impact Information Technology Resources.

    c. Establish the Information Technology Advisory Committee (ITAC) comprised of all members of the Information Security Advisory Committee (ISAC) and representatives of other County Departments/Divisions and Elected/Appointed Offices as needed. Establish procedures for the ITAC to coordinate the acquisition and use of Information Technology Resources across the County; ensure compatibility of County Information Technology Resources; enable the effective exchange of Electronic Information; and promote efficient use of County Information Technology Resources.

    d. Coordinate the goals and activities of the ITAC as appropriate with those of the ISAC.

C. Responsibilities of all ITAC members

1. Consult with the Information Technology Advisory Committee on the proposed purchase and implementations of all new Hardware and Equipment, Software or Internet Services that have the potential for increasing risks to security, systems' compatibilities or performance, facilitating the effective exchange of data, and improving the efficiency of County investments in Information Technology Resources. Issues related to Information Security shall be forwarded to the Information Security Advisory Committee for review.

2. Oversee compliance with this policy and related policies and procedures within their Department/Division or Elected/Appointed Office.

3. Coordinate the purchase and use of Information Technology Resources within their Department/Division or Elected/Appointed Office.

D. Provision of Critical Information Technology Resources

1. All ITAC member organizations, committee members and the committee as a whole shall ensure the following Information Technology Resources are provided to all Departments/Divisions and Elected/Appointed Offices:

   a. Electronic Mail
   Email services to every county computer user as required to support the functions of his or her position. Departments under the Board of County Commissioners are required to use the BIT approved email service(s) for internal business record communications unless otherwise prohibited by Federal, State, or other regulation or county policy. Appointed and Elected Offices are encouraged to use the BIT approved email service(s) and shall integrate any separate service(s) with the BIT approved email service(s) unless otherwise prohibited by Federal, State, or other regulation or county policy.

   b. Electronic Calendar
   Electronic calendaring and scheduling service(s)to every county computer user as required to support the functions of his or her position. Departments under the Board of County Commissioners are required to use the BIT approved calendaring and scheduling service(s) to schedule all business meetings and resources unless otherwise prohibited by Federal, State, or other regulation or county policy. Appointed and Elected Offices are encouraged to use the BIT approved calendaring and scheduling service(s) and shall integrate any separate service(s) unless otherwise prohibited by Federal, State, or other regulation or county policy.

   c. Mobile Devices
   Acquisition, delivery, maintenance and support of mobile devices to employees that have been approved for a county cell phone or authorized to use an employee owned cell phone per the Use of Information Technology Resources Policy. ITAC may establish procedures and standards regarding the acquisition, delivery, maintenance and support of mobile devices.

   d. Internet Access and Services
   Internet access to every county computer user as required for outbound and inbound county business subject to copyright, licensing, property rights, and privacy laws, rules and regulations. The availability, reliability and security of internet access and county Electronic Information stored, transmitted or processed by services provided over the Internet shall be ensured through compliance with relevant information security policies, procedures and standards.

   e. Remote Access
   The acquisition, delivery, maintenance, and security of access to the county's Information Technology Resources and Electronic Information from locations outside of the county's internal network in accordance with relevant information security policies, procedures and standards.

f. Data Backup and Restore
Data backup and restoration services for county Software and Electronic Information. The county shall not provide data backup and restore services for local disk drives on individual computers unless required for service to the public.

2. Problem Escalation and Management
Problems with Information Technology Resources or Electronic Information with the Departments/Divisions or Elected/Appointed Offices supported by an ITAC member shall be handled in accordance with their own local procedures and escalated to BIT or other ITAC members when needed. ITAC members will assist each other when needed to restore services.

3. Security

a. Physical Access

1) Physical access to the systems, networks, software services, and Electronic Information shall be limited to those authorized personnel who require access to perform assigned duties. Where systems are deployed in areas where controls may not completely restrict access to only authorized personnel, access shall be managed in accordance with established procedures.

2) All county owned or maintained servers shall be kept in a secured data center location in accordance with the requirements specified by the CIO.

b. Enhanced Access for IT Administrators
Enhanced system/service administrator access in compliance with relevant information security policies, procedures and standards.

c. Computer Facility Access and Protection Systems
Authorized information technology staff shall accompany all visitors, vendors and county staff who do not have the appropriate access credentials while accessing a computer room, data center or wiring closet. A record of all access to data centers and wiring closets by other than authorized information technology staff shall be maintained for a minimum of one year. Data centers shall have automatic fire protection systems installed. All systems within a data center shall be supported by a power conditioning uninterruptible power supply that provides adequate time to shut down systems per system hardware or software manufacturer's recommendations.