Title: Administrative Policy Information Technology Services	**Policy No.** Part 1, County Administration Chapter 2, Information Technology Services Section 5
	Effective Date October 16, 2007
Policy Custodian Information Technology Services Division	**Adoption/Revision Date** October 16, 2007 / May 24, 2013

Adopting Resolution(s): CC07-467

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

Purpose: To ensure compatibility with, access to, and protection of Jefferson County's Information Network (JCIN).

Procedure: Yes

Policy: Information Technology Services

A. Compatibility

1. All information technology investments for Jefferson County shall be reviewed in partnership with Information Technology Services (ITS) Division in accordance with the established ITS procedures.

2. ITS investments include but are not limited to:

   a. equipment,

   b. security protection mechanisms,

   c. enterprise servers and databases,

   d. mobile computing devices,

   e. proprietary and vendor supplied commercial-off-the-shelf applications, and

   f. desktop, laptop, printer and other related peripherals.

3. ITS shall also consider factors such as supportability and maintenance costs, and compliance with data protection and security requirements.

B. Access to JCIN

1. Electronic Mail

   a. An email account shall be made available to every county computer user.

b. Departments under the Board of County Commissioners are required to use the ITS designated email system for internal business record communications.

c. Agencies and Appointed and Elected Officials are encouraged to use the email application.

2. Electronic Calendar

a. An electronic calendaring and scheduling account shall be made available to every county computer user via an ITS-specified email system.

b. Departments under the Board of County Commissioners are required to schedule all meetings and resources through this system regardless of the type and nature of any other system in use.

c. Agencies and Appointed and Elected Officials are encouraged to use this application.

3. Wireless Devices

a. The acquisition, delivery, maintenance and support of Wireless devices shall be managed by ITS in accordance with ITS procedures.

b. The acquisition, delivery, maintenance and support of cell phones shall be managed by the Agency, Appointed of Elected Official or Department or Division Director who assigned the phone.

4. Internet
The Internet shall be made available to every county computer user for outbound and inbound county business subject to copyright, licensing, property rights, and privacy laws, rules and regulations.

5. Remote Access
ITS shall manage the acquisition, delivery, and maintenance.

C. Protection

1. ITS shall develop and manage a Security Program to prohibit the unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of electronic information stored on or transmitted over County computer systems and networks in order to maintain appropriate confidentiality, integrity, and availability.

2. Software
All software, regardless of origin, shall be approved for use by ITS. Only authorized software shall be used on County systems, PC's and networks.

3. Data Backup and Restore
   ITS shall provide data backup and restore services for County systems and networks, in accordance with ITS procedures and schedules. ITS shall not provide data backup and restore services for local disk drives on individual PCs.

4. Problem Escalation and Management
   System problems identified by a department or person outside of ITS shall be reported in accordance with established ITS procedure.

5. Physical Security
   ITS shall limit physical access to the system, network, and data 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 ITS procedures.

6. Internal Security
   Access to all infrastructure computing/networking devices [i.e., routers, hubs, firewalls, servers, etc.] shall be restricted. Access shall only be granted in accordance with established ITS procedures. Internal network connection points (ports) shall not be available in unmonitored or unrestricted publicly accessible areas.

7. Computer Facility Security

   a. An authorized ITS representative shall accompany all visitors, vendors and Jefferson County staff who do not have the appropriate access credentials while accessing a computer room, datacenter and wiring closets.

   b. A record of all access to data centers and wiring closets shall be maintained for a minimum of one year.

   c. Datacenters shall have automatic fire protection systems installed.

   d. All systems within the datacenter shall be supported by a power conditioning UPS that provides adequate time to shut down systems per system hardware or software manufacturer's recommendations.