Administrative Procedure
Alachua County, Florida

Bargaining Unit employees should review their appropriate Collective Bargaining Agreement (CBA) to determine if this policy applies to them. In case of a conflict between the applicable CBA and these policies, the provision in the CBA controls.

Procedure No.: AP 10-4 Effective: 8/1/2018

Revision No.: 1 Review Date: 7/26/2018

Technology and Usage

OVERVIEW: To define policies for use of Alachua County information technology resources.

SCOPE: This policy applies to all persons employed by the Board of County Commissioners.

PROVISIONS:

1. Definitions

    a. *Information Technology Resources* include (but are not limited to) procedures, hardware, equipment, facilities, software, and data that are designed, built, operated, acquired and maintained to collect, record, process, store, retrieve, display and transmit data.

    b. *Network* refers to the data connectivity maintained and supported by Alachua County.

2. General Rules

    a. The Information and Telecommunication Services Department (ITS) reserves the right to

        i. Monitor usage of information technology resources.

        ii. Authorize the installation and/or modification of any information technology resources.

        iii. Periodically perform software audits to ensure licensing compliance.

        iv. Limit, remove, filter, proxy, or otherwise manage access to the Internet in order to promote the continuing operation of the County's network and Internet presence.

    b. Facilities Management must review installation and/or modification of any information technology hardware resources that may have a substantial impact

on cooling, space or electrical requirements.

c. Installation of any information technology resources previously designated as surplus must be approved by the ITS department.

    i. Departments are solely responsible for maintaining maintenance contracts on any surplus equipment that is still in use but not covered under a warranty.

d. Using information technology resources for activities that are illegal, for personal gain, political activities, inappropriate, or offensive is prohibited.

e. Installation and/or modification of any information technology resources, not explicitly approved by ITS, is prohibited.

3. Network and Computer Passwords

    a. All employees shall secure their passwords.

    b. Passwords shall be changed every 90 days.

    c. Strong passwords are mandatory and must:

        i. Be eight or more characters in length.

        ii. Contain both upper and lower case letters.

        iii. Contain numeric digits.

        iv. Contain a special character

        v. Never be shared or written down on paper.

        vi. Be different from employee's personal accounts (i.e. personal email accounts and social networking sites.)

    d. Request for password changes can only be made by the user or in writing by supervisor.

    e. Do not use the "Remember Password" feature in applications like Internet Explorer and others.

    f. Do not use network passwords on public computers (i.e. internet café and hotel

lobbies) as these may contain key loggers.

g. If you suspect your account or password has been compromised, report it to your supervisor and the Helpdesk immediately.

h. “Scanning, Cracking, and Hacking" of the Network, including, but not limited to resources, assets, passwords and protocols is prohibited.

4. Software and Hardware Licensing

   a. End-user license agreements are used by software, hardware and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

   b. Compliance

      i. Departments must keep records of proof of purchase and licensing for all software and hardware purchased and maintain compliance with end-user agreements.

      ii. Employees must not install, upload, download, or use any unlicensed software.

      iii. All installed software and hardware must be owned / leased by Alachua County.

      iv. It is strictly prohibited to distribute or make copies of any software owned or licensed for use by Alachua County.

      v. Departments will also need to inventory software on all computers not regularly connected to the network including stand-alone PCs, laptops and mobile devices, as well as any equipment installed at off-site locations.

5. Preventing Malware

   a. Do not disable malware protection software on your computer.

   b. Do not install antivirus or anti-spyware applications without approval from ITS.

   c. Do not open unsolicited e-mail or websites which come from suspicious origin, or contain unexpected attachments.

6. Internet Usage

a. Access to and use of the Internet via the Network is routinely monitored and logged by ITS. Excess or inappropriate usage of the Internet will be reported to department directors.

b. Unauthorized use, downloading, or copying of copyrighted material, including music, movies and the like, is prohibited.

c. Public file sharing services must be approved by the ITS Security Team.

7. E-mail Procedures

a. E-mail received or sent by County owned mailboxes, in connection with the transaction of official business, is subject to state regulations for records retention and public record laws per current Florida State Statutes and County policy.

b. The transmitting of messages that may be considered offensive or disruptive is prohibited.

i. Offensive content includes, but is not limited to, harassing language or images based on protected status as defined by County Policy.

c. The County email system may not be used for:

i. Transmitting or receiving unauthorized copyrighted material.

ii. Promoting or soliciting personal political viewpoints.

iii. Transmitting commercial messages, employee solicitations, chain letters or messages of a political or religious nature.

iv. Soliciting funds or soliciting participation in outside organizations or promoting functions not related to County government unless authorized by the County Manager or designee.

d. Archiving E-mails.

i. All email messages will be stored by the ITS department in accordance with the Data Backup procedures listed in Section 8 of this policy.

ii. County employees are the official custodians of public records for any email messages that they produce or receive on behalf of County business.

e. Distribution Lists.

i. The preferred method of emailing large groups of employees is through the use of distribution list. Distribution lists are available via the Global Address Book of the County email system.

8. Data Backup and Storage

   a. User File and Directory Structure on NetApp SAN central storage is backed up daily via snap shots performed every 4 to 6 hours.

   b. All user data on the NetApp primary storage repository is backed up via daily/weekly/monthly backups to NDMP Tape backups.
      i. Tape retention is daily for 30 days, weekly for 12 months, monthly for 3 years.

   c. Server Backups.
      i. Physical servers are backed up via daily block level incremental backups and retained for 30 days.
      ii. Virtual Servers are backed up via daily backups performed by VEEAM. Weekly backups are moved to a secondary location for longer retention.

   d. Application servers (SQL, Exchange, SharePoint) are backed up utilizing "application aware" software.

   e. Financial System backups are performed daily.
      i. Daily backups are performed and stored on the NetApp Storage Area Network (SAN) system and copied to the Emergency Operation Center SAN system daily.
      ii. Backups for the past 2 weeks are kept and maintained at both the Wilson Building Server Room and Emergency Operations Center SAN systems.
      iii. Full system backups are handled by VEEAM on a daily basis.

   f. Once eligible for destruction, all backup media (tapes, disks, etc.) no longer in use is retired by destroying it in a manner that renders the media unreadable, unusable and incapable of recovering any data from it.

9. Vendor Access

   a. The department head of the County department for which the system is installed must approve vendor access prior to deployment.

   b. Prior to the installation of any system, vendors must request in writing the creation of their unique remote access accounts to the Alachua County ITS Security Manager for approval. Vendors will submit the following information:
      i. Vendor Organization

ii. Desired VPN account name
iii. Name and contact information (phone and email) for the employee associated to the account
iv. System(s) to be accessed
v. Anticipated time window of access required
vi. Detailed description of the anticipated activities (i.e. maintenance / updates / installations) to be performed

c. Vendors will utilize a unique account for each of their employees accessing the Alachua County network. Vendors will not share access accounts and passwords.

d. The account password will conform, at a minimum, to the requested ITS Strong Password Standard, including the 90 day password expiration policy.

e. Vendors will not login using service accounts.

f. Vendors are responsible to notify in writing to the Alachua County Security Manager when an employee of the vendor no longer needs access to the Alachua County network.

g. All remote access must be authenticated and encrypted through the Alachua County Virtual Private Network (VPN).

h. No vendor account will have administrator or elevated privilege access to the system they support, unless it is approved by the ITS Security Manager or the ITS Director.

i. Vendor accounts will have access only to the systems that they support or maintain and that have been approved by the department head of the County agency involved and ITS. Account specific profiles will be created for VPN access and will only be allowed to access specific devices or systems.

j. ITS will be responsible for enabling/disabling accounts and monitoring vendor access to County networks, applications and systems.

k. Any violation to the above items will result in immediate termination of the user account and remote access privileges.

10. Vendor Installed Equipment

a. All vendor equipment installed in the Alachua County Network must comply with security standards established by the Alachua County Security Manager. ITS will seek to eliminate any potential exposure of the County networks

resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of the Alachua County networks, data, systems and applications.

b. Vendor must provide separate administrative access account to the Alachua County Security Manager for any equipment installed in the county's network, before equipment is attached to the county network.

c. Alachua County will quarantine or remove any equipment that does not comply with the equipment security requirements or any equipment that compromises the security of the Alachua County network.

11. Remote Access

a. Do not use public computers, such as public library computers, school/college computers, and those computers that are rented (i.e., at an Internet Café) for remote access to the Network.

b. All remote Network connections provided to employees, vendors, contractors, or non-employees must be approved by the ITS Director, or designee.

i. Software requirements for remote network access to the Network

(1) Computer or network devices that establish a remote access connection to the Network must have:

(a) An operating system currently patch supported by the vendor
(b) Operational, up-to-date, anti-virus software installed.

(c) Service packs and critical updates installed.

(d) Firewall activated.

(e) Internet Connection Sharing turned off.

(2) Third Party Remote Access Software.

(a) The use of third-party software or hardware to initiate a connection to an employee's computer that resides within the Alachua County Network must be approved by ITS.

(b) The use of third party software to publish content, or make

available directly to the internet any data from a County computer or Network connected device without the prior approval of ITS is prohibited.

b. It is the responsibility of remote access users to ensure that unauthorized users are not allowed access to the Network via their remote connection.

12. Social Networking Procedures

a. Department Directors must approve, in writing, the creation of accounts for posting County content on non-County owned social networking sites.

b. The name of a site will include Alachua County, and the division or program name. Only the County's main site which is maintained by the County's Communications Office will feature the County's official logo.

c. The Department Director is responsible for assuring:

i. Information is current, accurate, appropriate, professional and courteous.

ii. Timely response to comments received from citizens on social networking sites.

iii. Backing up information created on social networking sites.

iv. Deleting social networking sites that are dormant.

v. Retaining public records created by the social networking site.

_____ _____

County Manager County Attorney