Information Technology Division

Computing Security Procedures

Last Revised Date: August 19, 2019

TABLE OF CONTENTS

Contacts

Main Contact

This document will make references to the contacts found below. Contact information may also be found on ENN. If you are unable to locate someone or have a question, always feel free to contact the IT Support Desk for assistance**.**

IT Support Desk phone number	740-5222 or x 15222
IT Support Desk email	IT_SupportDesk@volusia.org

IT Security Officer phone number	740-5222 or x 15222
IT Security Officer email	IT_SupportDesk@volusia.org

Other Contacts

Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Sheriff's Office IT phone number	x 13501
Sheriff's Office IT email	infosys@vcso.us

Elections IT contact	Gary Buchanan
Elections IT phone number	x 15801
Elections IT email	gbuchanan@volusia.org

Library Services contact	Annie Powers
Library Services IT phone number	x 11216
Library Services IT email	apowers@volusia.org

Property Appraiser IT contact	Mark James
Property Appraiser IT phone number	x 15511
Property Appraiser IT email	mjames@volusia.org

Objectives, Scope, and Compliance

Objectives of Procedures

The primary objective of the *Computing Security Procedures* is to protect Volusia County (County) Computing Resources from being intentionally or unintentionally compromised. The secondary objective is to establish responsibility and accountability for the security of County Computing Resources.

Scope of Procedures

These procedures apply to all Users of County Computing Resources.

Compliance

Compliance with the Volusia County *Computing Security Procedures* is mandatory and considered a condition of continued employment. Failure to comply with the *Computing Security Procedures* may result in disciplinary action.

All vendors, contractors, interns, volunteers, and consultants performing work on behalf of the County are considered Users and are required to follow the *Computing Security Procedures* when utilizing County Computing Resources. Failure to follow the *Computing Security Procedures* may be considered a breach of contract.

Department/division management is responsible for enforcement of these Procedures to protect County Computing Resources from unauthorized access, compromise, use, destruction, or modification. For contracted work, it is the responsibility of the prime contractor to enforce the *Computing Security Procedures* with respect to contractor's staff and subcontractors.

Departments and divisions may implement more stringent Procedures in addition to these minimum Procedures.

County Computer Systems store, process, and transmit sensitive information, including criminal justice, personally identifiable information, protected health information, and critical infrastructure information. Each type of sensitive information includes additional protection requirements that flow down to the County through Federal statutes, regulations and policy. Failure to follow the *Computing Security Procedures* may result in a criminal offense as described in the Florida Computer Crimes Act (Chapter 815, Florida Statutes) and/or civil or criminal penalties for mishandling of sensitive information governed by Federal statutes, regulations, and policy.

Definition of Terms

Definitions are included in Appendix A: Definition of Terms

Avoiding Malware, Viruses and Hoaxes

Background

Computer malware (e.g., viruses, worms, spyware, ransomware, Trojan horses, rootkits, etc.) are programs designed to do damage or other unwanted actions to a computer including making unauthorized changes to applications, files, email, networks, and data. Malware can cause the destruction and/or corruption of County Computing Resources, compromise information, and can prevent Users from completing work. Intentionally introducing a virus, worm, Trojan horse, or other malicious program to a network is a criminal offense. For more information on criminal offenses, see the Florida Computer Crimes Act (Chapter 815, Florida Statutes).

Similar in nature, hoaxes warning of malware outbreaks are sent via email or other similar communication methods. Along with the warning are instructions to prevent infection. These instructions typically involve deleting files and forwarding the warning to friends and relatives. If you delete these files your system will no longer function correctly.

Ransomware is a type of malware that prevents or limits Users from accessing their system, either by locking the system's screen or by locking the Users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decrypt key. Users may encounter this threat through a variety of means. Ransomware can be downloaded onto systems when unwitting users visit malicious or compromised websites. It can also be delivered as attachments to email, through malicious web pages in advertisements, or be downloaded by other malware.

Phishing is another form of hoax that utilizes emails, texts, or phones to solicit personal information or cause a person to visit fraudulent web sites. In Phishing, the end goals are theft of your identity and money through the acquisition of information such as account passwords and other confidential data, or the ability to gain unauthorized access to computer systems based on information disclosed during the phishing expedition.

Cyber criminals are writing viruses that specifically use or target removable media (USB drives, portable hard drives, smartphone memory). If you plug in an infected USB drive into a work or home computer, a virus could be uploaded and potentially cripple the machine and others on the network. Removable media can already be infected at the time of purchase if quality control measures are not adequate during the manufacturing or supply chain process. Only use removable media from trusted sources.

Procedure

All County Computing Equipment, including but not limited to workstations, laptops, tablets, and servers, will be provided with anti-virus protection. The anti-virus program will be running at all times and set to automatically apply updated virus protections released by the anti-virus vendor. The operating systems on these devices will be updated using either Information Technology’s Windows update server or using the operating system’s vendor site.

All non-County Computing Equipment with authorized access to the County’s network is required to be equipped with an approved anti-virus program. The anti-virus program will be running at all times and set to automatically apply updated virus protections released by the anti-virus vendor.

Standard

Information Technology uses multiple anti-virus servers running enterprise class anti-virus software. The anti-virus servers are authorized by the anti-virus software vendor to download anti-virus updates over a secured Internet connection. When the vendor posts an update, the anti-virus servers automatically download the update. All County Computing Equipment is initially set up to automatically download anti-virus updates from the anti-virus servers when they are posted.

All non-County Computing Equipment used to perform county job functions will be configured with continuously running anti-virus software as considered necessary by Information Technology and department management.

Regardless of who owns or provides Computing Equipment used to perform county job functions, Users shall not install any applications, change any configurations, tamper with, disable or take any other action that interferes with anti-malware software and operating system updates.

Guidelines

User Responsibilities

- Be aware and do not ignore the symptoms of a virus or other malware. These symptoms include slow workstation response, system failure, system prompts, anti-virus software messages, or automatic reboots.

- Report malware symptoms, anti-virus software warnings, and suspected hoaxes and Phishing to the Information Technology Support Desk. DO NOT FORWARD THE VIRUS. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

- Download files, attach devices, and use media from trusted sources only.

- Run anti-virus scans on all files and media downloaded to workstations, laptops, tablets, servers, or other County Computing Resources, even those from a trusted source. This includes files stored on a USB drive, CD, DVD, diskette, other storage media, and the Internet. How-to instructions are available on Information Technology's ENN home page under the training section.

- Ensure anti-virus software is running on your Computing Equipment. How-to instructions are available on Information Technology's ENN home page under Resources, Reference Library, How To, Verifying Workstation Anti-Virus.

- Follow instructions for avoiding or fixing a virus infection only if provided by the Information Technology Support Desk, department/division support staff, ENN Hot News, or a workstation analyst. Forward any instructions you receive from other sources to the Information Technology Support Desk or local department/division support staff for review and validation.

- Ensure an approved anti-virus program is installed, enabled and up to date on non-County equipment prior to connecting equipment to County equipment or utilizing County data.

Approved Anti-Virus Guidelines for Home PCs.
http://ennprod/informationtechnology/cabinet/standards/Anti_Virus_Guidelines.pdf

- Purchase USB drives and other removable storage from reputable vendors only. An unusually low price could indicate that a USB drive may be counterfeit or infected with malware.

- Do not connect removable drives from unknown sources (e.g. found on floor, received in the mail unsolicited, promotional giveaways) to County equipment.

- Do not purchase USB drives unless they are on the County's approved list. For a list of approved USB drives:

Approved USB drives
http://ennprod/informationtechnology/cabinet/standards/Jump_Drive_Procurement_Guidelines.PDF

- Avoid Phishing scams by carefully reviewing email prior to clicking on links or following questionable instructions even when valid-looking logos are used. Phishing scams may contain grammar mistakes, request personal information, and reference transactions pertaining to deliveries, bank accounts, or the IRS as a way to appear legitimate. Contact the Information Technology Support Desk if further assistance is needed. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

- For more information on phishing, visit the Federal Trade Commission website. The Federal Trade Commission is responsible for policing the Internet with respect to fraud.

Federal Trade Commission phishing article
http://www.consumer.ftc.gov/articles/0003-phishing

Information Technology Responsibilities

- Install and maintain appropriate anti-malware/anti-virus protection software as considered necessary by Information Technology on all County Computing Equipment. Local IT support within the Sheriff's Office, Elections, Library Services, and Property Appraiser will install and maintain appropriate anti-malware/anti-virus protection software on all equipment under their control.

- Review anti-malware logs daily.

- Immediately contain and eradicate any malware infections.

- Maintain anti-malware protection for the County email system that automatically identifies and deletes or quarantines infected email or attachments. Local IT support within the Sheriff's Office is responsible for the Sheriff's email anti-virus protection.

- Notify Users about widespread malware threats and known hoaxes that may impact the County.

- Install operating system software security updates on County Computing Equipment. Local IT support within the Sheriff's Office, Elections, and Library Services, will install and maintain appropriate updates on all equipment under their control.

- Respond in a timely manner to any type of malware alert and take corrective action. Local IT support within the Sheriff's Office, Elections, Library Services, and Property Appraiser will respond in a timely manner to any type of malware alert and take corrective action on all equipment under their control.

Disposal of Computing Equipment and Media

Background

County Computing Equipment and physical and electronic media may contain software, applications, and data used to provide County services. If not removed upon disposal, sensitive information such as criminal justice information (CJI), health information, Personally Identifiable Information (PII), or passwords may pose a security risk. Physical media includes printouts, printed imagery and other paper documents containing sensitive information. Electronic media includes but is not limited to hard-drives, tape cartridges, CDs, DVDs, printer ribbons, USB drives, printer and copier hard-drives, SIM cards and smartphones. Federal regulations detail the proper handling and disposal of physical and electronic media. These regulations ensure compliance with Health Information Portability and Accountability Act (HIPAA) and CJI mandates and are consistent with the intent of Florida Statute to protect people's personal information.

HIPAA laws and regulations
https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/

CJIS Security Policy Resource Center
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Additionally, Florida Statutes protecting personal and health information may also be relevant when County activities are governed by the State, such as oversight and control of the elections process, critical infrastructure and healthcare. Adherence to this procedure also should enable compliance with Federal and State requirements.

Procedure

When no longer needed, physical and electronic media used to process, store and/or transmit County data shall be properly disposed of or repurposed in accordance with measures established by the County of Volusia.

a. Physical media (printouts, printed documents, printed imagery, printed facsimile) containing CJI, HIPAA or sensitive data shall be disposed of by one of the following methods:
    i. Shredding using County of Volusia cross-cut shredders.
    ii. Placing CJI in locked shredding bins for the County's authorized contractor to come onsite and shred, witnessed by County personnel throughout the entire process.
    iii. Placing HIPAA and non-CJI sensitive data in locked shredding bins for the County's authorized contractor to pick up and shred.
    iv. Incineration of sensitive data at a contractor incineration site.

b. Electronic media (hard disk drives, tape cartridges, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be prepared for disposal or reuse by one of the following methods:
    i. Overwriting (at least 3 times): This effective method clears data from magnetic media. As the name implies, overwriting uses a program to write binary digits (1 and 0) onto the location of the media where the file to be sanitized is located. Electronic media may now be sent to auction or reused.
    ii. Degaussing: This method magnetically erases data from magnetic media. Degaussing using strong magnets designed for degaussing purposes or electric degaussing methods

are acceptable. Common magnets, such as those used to hang a picture on a wall are weak and cannot effectively degauss magnetic media.

iii. Destruction: Electronic media can be physically dismantled by methods of crushing, disassembling, mutilation, incineration, etc., ensuring that the platters have been physically destroyed so that no data can be pulled. This method may be performed by CJI Authorized Personnel.

CJI Authorized Personnel must witness and log both physical and electronic media disposal when CJI is involved.

Standards

Shredding is only to be used for disposal of paper-based physical media. Electronic media being disposed of will be rendered non-usable by physical means. CDs, DVDs, floppy disks, and like type of electronic media will destroyed by incineration, mutilation (e.g., crushed, impaled, etc.), or chemical decomposition. Hard disk drives, USB drives, memory cards, and like media will be erased using a degausser approved by the Federal Government or physically destroyed through mutilation or incineration.

Electronic media being repurposed will be overwritten at least three times before being repurposed.

Guidelines

User Responsibilities

a. Ensure all data have been appropriately preserved (e.g., backed up, copied, printed out, etc.) consistent with County records management retention requirements to comply with Florida's Sunshine law.

b. Shred paper-based physical media containing CJI, HIPAA or other sensitive information.

c. Format using software that meets Department of Defense standards for all portable electronic storage media prior to repurposing. Destroy by physical means all non-usable portable electronic media including, but not limited to, disk drives, USB drives, diskettes, CDs, DVDs, and tape prior to disposal.

d. Contact the Information Technology Support Desk to arrange for a workstation analyst to destroy data on Computing Equipment prior to repurposing or disposal.

e. For county owned smartphones, the following at a minimum needs to be done. For a comprehensive list and detailed instructions, see the below link.
    1. Backup all data and connections, including text/instant messages to comply with Florida's Sunshine law,
    2. Unpair any connected devices,
    3. Turn off and sign out of any message applications,
    4. Sign out of all social media applications,
    5. Erase all contents and settings,
    6. Encrypt the data. Encrypting the data prior to performing the factory reset will protect residual data residing in storage,
    7. Perform a factory reset,
    8. Verify all settings are cleared,

9. Provide your supervisor with the device lock codes and any associated business user-ids and passwords that may be needed for re-provisioning of the device if you will no longer be utilizing the device or associated accounts for county business.
10. Remove the SIM card and any micro SD cards prior to disposing of or trading in the phone.

Smart Phone Reset Guide
http://ennprod/informationtechnology/cabinet/howtoguides/Smartphone_Reset_Guide.pdf

f. Contact the Information Technology Support Desk if further assistance is needed. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Information Technology Responsibilities

a. Prepare drives for disposal using one of the following methods:

Method of Drive Disposal	Approved Drive Handling
PC replacement end-of-life (spinning drive and SSD)	Wipe using Department of Defense Sanitation Standards
Internal retention and repurpose (spinning drive and SSD)	Wipe using Department of Defense Sanitation Standards
Device disposal (spinning drive)	Wipe using Department of Defense Sanitation Standards, degauss or physically destroy
Device disposal (SSD)	Wipe using Department of Defense Sanitation Standards or physically destroy

b. Destroy by physical means all inoperable portable electronic media including but not limited to disk drives, USB drives, diskettes, CDs, DVDs and tape prior to disposal.

c. Disposal of any electronic media that previously contained CJI and HIPAA information shall be witnessed or carried out by CJI Authorized Personnel. Destruction records are required for CJI information and shall be maintained for two (2) years within the IT Division folder structure called ITD:\IT_Operational\CJI_Hard_Drive_Destruction. The records shall indicate the date of the destruction, identify the material destroyed, destruction method, and be signed by the individuals designated to destroy and witness the destruction. CJI Authorized Personnel serving as destruction witnesses shall be required to know, through their personal knowledge, that such material was destroyed.

Regulations and requirements regarding handling of electronic media are expected to change over time. IT personnel are responsible for ensuring continued compliance with governing regulations when handling any electronic media that contains HIPAA, CJI or any other sensitive data. Information Technology (IT) systems that have been used to process, store or transmit CJI and/or sensitive information shall not be released from the County's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Employee Remote Access

Background

While offering potential benefits, remote access to County resources introduces risks to the security of applications and data.

County Information Technology professionals cannot control the operating system, security settings, installation of security patches, specialized security software, or physical access to an employee-owned PC, laptop, tablet, or smartphone. Employee-owned computing equipment is considered unmanaged and unsecure.

Each remote access account and access point to the County network increases the security risk. Management is asked to grant remote access requests only where use will significantly benefit County operations.

Procedure

- Remote access will be provided in a secure manner and at the discretion of an employee's division manager and with Information Technology concurrence. Under no circumstance is it permissible to remotely access any Computing Equipment which can access criminal justice data (CJI) unless acceptable encryption methods are in place. The Florida Department of Law Enforcement (FDLE) and Federal Bureau of Investigation (FBI) have strict policies in place regarding this type of access.

- Management will ensure that remote access is a significant benefit to County operations.

- Remote access will be gained only through access points under the management of County Information Technology or approved by County Information Technology.

- Employee workstations directly attached to the County network and configured to permit remote access without management approval are a violation of this Procedure.

- Remote access to computer resources accessing CJI requires advanced authentication.

- The County is not responsible for the configuration, repair, or diagnosis of non-County Computing Equipment.

Standard

Remote access to County email does not require a User to have access to the County network. All employees with County GroupWise email accounts may use this link to securely access email via the Internet:

GroupWise secure webmail
https://webmail.vcgov.org

With management approval, County and employee-owned Computing Equipment may be provided access to the GroupWise email system in an active synchronization mode where appointments and

email are pushed to the device. Management shall determine the need, and work with Information Technology to approve these requests.

Workstations, by default, will be deployed with remote access disabled.

The County maintains a virtual private network (VPN) solution to provide secure remote access by vendors and employees. The VPN solution provides for the authentication of Users, encryption of communication, and authorization of selected Computing Resources by logon.

Guidelines

User Responsibilities

- Upon establishing a VPN connection on a private device, connect to a County Computing Resource first, such as your County desktop PC, instead of connecting directly to the file system.
- Safeguard hardware or software provided by the County.
- Provide personal Internet accounts, phone lines, cable connections, remote wiring, etc., required at home or other areas outside of County premises.
- Install and maintain appropriate security software including, but not limited to anti-virus software, security patches, and automatic software updates.

Approved Anti-Virus Guidelines for Home PCs.
http://ennprod/informationtechnology/cabinet/standards/Anti_Virus_Guidelines.pdf

- Provide for the maintenance, diagnosis, and repair of non-County owned hardware and software.
- Use discretion as laws regarding public records may apply to remotely attached workstations and devices including your employee-owned Computing Equipment.
- Ensure all County data, including public records, are properly safeguarded and not stored on a personal device.
- Ensure that remote access accounts, user accounts, and equipment are not available to unauthorized individuals. Prevent access to these accounts by spouse, children, or others that may have physical access to the equipment.
- Lock the screen with a password if the Computing Equipment is left unattended.
- Contact the Information Technology Support Desk if further assistance is needed. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Department/Division Liaison Responsibilities

- Contact the Information Technology Support Desk upon receiving division director authorization to request remote access for an employee.

Information Technology Responsibilities

- Review and respond to remote access requests within five business days.
- Maintain the necessary remote access points, firewalls, and security measures to aid in keeping the networks secure.
- Implement and maintain remote access accounts limiting external Users to only those resources required to perform their duties.
- Provide Users guidance in configuration, access, and use of remote access.
- Provide for the maintenance, diagnosis, and repair of County owned hardware and software.
- Provide quarterly reports to department/division liaisons or their designees listing remote access accounts for verification that information is accurate. Disable accounts where appropriate.
- Provide encryption software that uses FIPS 140-2 validated cryptographic modules to all remote users that require County data be encrypted to meet regulatory compliance.

Equipment, Data, and Media

Background

Computer hardware, software, and networks are the property of Volusia County and are provided for the purpose of conducting County business. Incidental and occasional personal use may be permitted by management as outlined in the Volusia County Communications Policy.

Volusia County Communications Policy
http://ennprod.covdnssrv.co.volusia.fl.us/communityinfo/Communications-Policy.pdf

News agencies frequently highlight events where a laptop or other electronic media carrying personal information on hundreds of thousands of employees, retirees, applicants, or other files are stolen or lost. The information lost or stolen is frequently more than enough to pose a potential threat of identity theft and discredits the organization.

Procedure

- Access to Computing Resources shall be restricted to authorized Users. Authorization to use Computing Resources will be limited to the User's need to fulfill job requirements. Management within the department responsible for the application, data, and/or equipment is responsible for authorizing all User access. Security will be configured to adhere to the standards and conventional practices of internal and external auditors in accordance with the principle of least privilege.

- Access to all computer resources requires secure authentication provided by Information Technology. Where advanced authentication is required, such as accessing CJI data, computer users shall use advanced authentication security measures as deployed by Information Technology. The advanced authentication system will be compliant with the FBI Computing Security Policy. Examples include hardware tokens, software tokens, certificates, and other approved measures.

CJIS Security Policy Resource Center
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

- County management retains the right to inspect any and all files, equipment, and logs created and/or stored on County Computing Equipment.

- It is the employee's or vendor's responsibility to protect from loss or theft any data in their possession. Data encryption is required when removing laptops or electronic media from County facilities if the data files contain sensitive or confidential information such as social security numbers or protected health information.

- Installation of all computer software on County Computing Equipment shall be authorized by Information Technology.

Standards

- Software installation on County Computing Equipment will be performed by qualified and authorized staff. Staff will follow industry-accepted installation and verification practices to ensure that software is installed and configured to provide maximum security and reliability.

- Windows operating system password protected screen savers will be configured to activate after fifteen minutes of inactivity on workstations and laptop computers. On a case-by-case basis management can approve extending the time of inactivity in accordance with the CJIS Security Policy Section 5.5.5 Session Lock and/or disabling the screen saver timeout. Examples of where this would be valid are a kiosk, a secure front counter device, and a surveillance monitor.

Guidelines

User Responsibilities

- Be alert to the presence of unauthorized persons in the work area. Contact a supervisor, building security, and/or law enforcement if a person entering the work area does not provide credentials, seems suspicious, or poses a possible threat.

- Store and secure USB drives, CDs, DVDs, diskettes, or other media out of sight when not in use. Media containing highly sensitive or confidential data shall be appropriately secured, and when warranted, the data encrypted. When in doubt, request Information Technology or department/division assistance on encryption and proper protection.

- Use County Approved Encryption Methods when accessing or storing County data that must be protected to meet regulatory requirements. It is the User's responsibility to identify and know which data are required to be encrypted.

- Protect Computing Resources including desktops, laptops, tablets, smartphones, USB drives, CDs, DVDs, diskettes, and media from environmental hazards such as direct sunlight, magnetic fields, food, smoke, liquids, humidity, dirt, dust, sand, drops/bangs, power surges/cuts, and extreme heat or cold. Users who neglect this may be accountable for any resulting loss or damage.

- Contact Information Technology Support Desk for equipment recommendations and approval (e.g. laptops, printers, GPS units, plotters).

- Contact Information Technology Support Desk for equipment installations, disconnections, modifications, relocations, and software installations. This includes printers and other peripherals.

- Follow this Procedure and any additional departmental procedures regarding the use of Computing Resources including data outside of County offices.

- Follow this Procedure and any additional departmental procedures regarding the downloading of data. Download data from trusted sources only.

- Before downloading files or using files or data from even a trusted source, check that the anti-virus software on your computing equipment is current and operational. Scan all downloaded material using anti-virus software prior to use. How-to instructions are available on Information Technology's ENN home page under the training section.

- Do not take any actions to disable or prevent screen saver from activating on a workstation. Contact Information Technology Support Desk if screen saver does not activate on a workstation after fifteen minutes of inactivity. On a case by case basis management can approve extending the time of inactivity in accordance with the CJIS Security Policy Section 5.5.5 Session Lock and/or disabling the screen saver timeout.

- Lock the password protected screen saver whenever County Computing Equipment is left unattended.

- Shut down and power off your workstation properly at end of each workday.

- Lock the password protected screen saver at end of each workday on workstations that have been approved to remain powered on continuously.

- Secure, monitor, and protect portable Computing Resources, which are more susceptible to loss, theft, and damage.

- Report any lost or stolen equipment and/or media immediately to Information Technology Support Desk and direct supervisor. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

- Contact the Information Technology Support Desk if further assistance is needed. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Information Technology Responsibilities

- Set up a password protected screen saver included with the operating system on all County-owned workstations, tablets and laptops. The screen saver will be set to come on after a maximum period of inactivity. On a case-by-case basis management can approve extending the time of inactivity in accordance with the CJIS Security Policy Section 5.5.5 Session Lock and/or disabling the screen saver timeout. Mobile devices should be set to power down the screen quickly when not in use and have a lock code.

CJIS Security Policy Resource Center
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Maximum period of inactivity until screensaver activated	15 minutes

- Configure County Computing Equipment to require a password on devices at system startup and when unlocking the screen saver.

- Provide equipment and software consultations, recommendations, and approvals.

- Install County Computing Equipment with appropriate software security measures including, but not limited to antivirus software, patches, automatic software updates, passwords, and/or remote management software.

- Install, disconnect, and modify hardware and software as requested by departments/divisions through the Information Technology Support Desk.

- Provide consultation on appropriate use and data encryption.

- Provide an on-screen notification to users who access CJI data that usage of County Computing Equipment shall be by authorized individuals only and that any such usage may be monitored.

Purchasing Responsibilities

- Contact Information Technology for review and approval of Computing Resource purchase requests and to participate in solicitation projects that include Computing Resource acquisition or implementation.

Internet

Background

The use of the Internet has become commonplace throughout the organization as a means of conducting business. While connecting to the Internet can be a tremendous asset to County government, it also heightens the exposure of County Computing Equipment to unauthorized access and tampering. Industry statistics show that computing devices connected to the Internet pose an increased likelihood of being infected with spyware programs, viruses, and other malware. Most recently, increasing numbers of ransomware attacks occur through users clicking on a compromised websites.

The malicious programs can result in data corruption or damage to computer systems. For example, in 2018 Atlanta encountered a ransomware attack resulting in more than a third of Atlanta's 424 applications becoming unavailable, close to 30% of which were "mission critical". The City Attorney's office lost the ability to use all but six of its 77 computers and 10 years' worth of documents, while the police lost their dash cam recordings, compromising pending DUI cases. Some estimates put the cost at $17 million to recover.

Procedure

Management and staff will ensure the Internet is used in a manner that minimizes security risks to the County.

Standard

Internet access will be provided to employees as part of the County Standard for County Computing Equipment unless department/division management directs Information Technology otherwise.

Guidelines

User Responsibilities

- Abide by the Volusia County Communications Policy regarding Internet use.

Volusia County Communications Policy
http://ennprod.covdnssrv.co.volusia.fl.us/communityinfo/Communications-Policy.pdf

- Ensure that any transactions involving sensitive information such as protected health information, passwords, and social security numbers are conducted with Trusted Sites via encrypted/secure connections. An Internet address that starts with HTTPS instead of HTTP indicates that the connection is encrypted. Use the lock icon on the browser to review the site validity and certificate authority.

- Use VeriSign, GoDaddy, and Symantec protected sites or a similar security offering for transactions involving sensitive information such as protected health information, passwords, and social security numbers.

- Do not click on web links and articles that are not related to County business. While occasional personal use may be approved by management, do not use County Computing Resource to access internet web pages that may be compromised such as those displaying eye catching articles such as “Did Mark Zuckerberg Buy a $150 Million Yacht?” or that advertise products at too good to be true prices.

- Do not use instant messaging from a Volusia County Computing Resource.

- Check that the antivirus software on your County Computing Equipment is current and operational before downloading and using files or data from a trusted source. How-to instructions are available on Information Technology’s ENN home page under the training section.

- Scan all downloaded material using antivirus software prior to use. How-to instructions are available on Information Technology’s ENN home page under the training section.

- Contact the Information Technology Support Desk if further assistance is needed. Employees of the Sheriff’s Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Information Technology Responsibilities

- Deploy new County Computing Equipment with Internet access unless directed otherwise by department/division management.

- Maintain County-wide Internet access services.

- Install and maintain appropriate software security measures including, but not limited to antivirus software, security patches, and automatic software updates.

- Block access to restricted sites and services as identified.

Network Equipment

Background

The advent of inexpensive and easy to install consumer networking equipment has introduced an increased potential for exposing County resources to security breaches.

Information Technology is responsible for all connections to the County Network.

Consumer wireless network hubs, wired hubs, and network diagnostic equipment are easily purchased at retail electronics stores for under a hundred dollars. These hubs and wireless local area network (WLAN) devices are intended for household use. Consumer products do not incorporate the security Standards necessary to protect the County network, Computing Resources, and data and should not be used.

Procedure

All access and access points to the County Network will be reviewed and approved by Information Technology.

All network access points (wired and wireless) and network equipment deployed or used within County facilities or connected to the County Network must be approved by Information Technology before installation.

Standards

Information Technology maintains Standards for equipment that is appropriate for use on the County Network and in County facilities.

Residential products are not appropriate for use on the County network.

Guidelines

User Responsibilities

- Contact the Information Technology Support Desk with all network requests and WLAN requirements prior to implementation.
- Install only authorized network or WLAN equipment on the County network.
- Contact Information Technology Support Desk before using any diagnostic equipment or software on the County Network.
- Report suspicious network equipment on the County Network to the Information Technology Support Desk. This would include simply seeing a consumer wireless or wired network hub in the general work area.
- Monitor the activities of vendors, contractors, employees, interns, and volunteers to ensure they comply with this Procedure.

- Use County provided wireless access points when available to connect County Computing Resources. Under no circumstance is any CJI data to be transmitted via any wireless access point.

- Use caution when connecting County Computing Resources to wired or wireless networks outside of the County Network. For example, Internet services at airports, restaurants, and hotels are normally not as secure as the closed County Network.

- Contact the Information Technology Support Desk if further assistance is needed. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Information Technology Responsibilities

- Provide a reliable, secure, and documented network.

- Approve all network requests and WLAN solutions before implementation.

- Install and configure County networking and WLAN solutions.

- Investigate and resolve any identified unauthorized access points on the network.

- Remove unauthorized access points on the network and report the removal to the department/division liaison and the IT Support Desk. The IT Support Desk will report this event to the Information Technology Director and IT Security Officer.

Passwords

Background

The confidentiality, integrity, and availability of data stored on County computer systems must be protected by passwords to ensure only authorized individuals have access. Access to County systems is restricted to only those functions required for each individual to perform their County duties.

Information Technology, and the IT industry in general, no longer recommend the use of passwords. IT recommends the use of passphrases, which are considerably longer. However, many systems are as of yet unable to support lengthy passphrases, leading to a transitionary period.

The following is an example of a password: **family123**

This particular password has an estimated cracking time of 74 milliseconds. An eye blink is 300 to 400 milliseconds, meaning that this password can be cracked faster than you can blink.

A passphrase is a series of three or four unrelated words, such as: **TransmitDrainOverseeBird**

The above passphrase has an estimated cracking time of 110 centuries. The increase in cracking time is largely due to the increased length of the password and the fact that the words are unrelated.

In those systems where it is possible to use them, IT recommends using at least three unrelated words as a passphrase. The key is to use unrelated words, which should not form a proper sentence or be grammatically correct. Password crackers already search for phrases from movies and books, as well as common phrases. Words that naturally go together and have meaning should not be used. Although the length of a passphrase gives it security, a number, capital letters, or symbol thrown in will strengthen the passphrase even more.

Procedure

User passwords are a key to the protection of County resources. Users are responsible for the protection and maintenance of their passwords.

Strong passwords will be maintained by all individuals accessing County applications or Computing Resources.

Passwords will be changed anytime the individual suspects someone has unauthorized knowledge of their password.

Standards

Passwords or passphrases shall be a minimum length and contain other attributes, as defined below. Longer and more complex passwords are recommended including the use of special characters and mixed upper and lower case letters where supported.

Passwords will not be composed of easily guessed content or common words found in a dictionary. Do not use your name or the names of relatives, friends, or pets as part of the password. Do not use easily seen or guessed strings of letters on the keyboard like 12345678 or QWERTY00.

The nature and value of the application being accessed will determine the need, length and complexity for a password. As an example, email, human resources, finance, criminal justice, and land information applications all require passwords for use, while use of the ENN phone book does not.

It is recommended, and in some cases required, that different applications have unique passwords.

In those systems where it is possible, use passphrases instead of passwords. In those systems where passphrases are not an option, the following minimum requirements hold:

Minimum length of password	8 characters
Minimum number of digits in password	1
Upper case character	1
Lower case character	1
Special character	1
Not be the same as the User ID	
Expire within a maximum of 90 calendar days Not be identical to the previous ten (10) passwords	
Not to be displayed when entered	
Maximum limit of 5 consecutive invalid access attempts. In such case, the account will be locked for a 10 minute time period, unless unlocked by an administrator.	

Guidelines

User Responsibilities

- Passwords should not be written down. However, if deemed necessary they shall be properly secured.
- User shall not use Internet-based password managers. Password managers that store data on a County file server are acceptable.
- Ensure that access to Computing Resources can be gained in the event of an emergency. Ensure your supervisor has access to passwords that cannot be reset by system administrators such as those protecting Microsoft Excel/Word documents.
- Review and follow instructions for resetting network, GroupWise email, and other passwords. How-to instructions are available on Information Technology's ENN home page under the training section.

Do	Don't
Contact the Information Technology Support Desk immediately if a password is compromised and change the password	Use personal information like pets' and children's names, last names, birthdays, hobbies, addresses, nicknames, etc. or common words found in a dictionary as a password

Choose a passphrase or password that is easy to remember but hard to guess	Use same password as on your home PC, home email account, or personal mobile devices and networks (e.g., smartphone, automobile WiFi)
Follow the password standard defined above	Click “Remember Password?” on your workstation if you are prompted
Be aware that certain applications do or do not differentiate upper and lower case	Use special combinations with ALT, CTRL or Option keys
Verify the identity of IT Support Staff or workstation technicians who may ask you to enter your password to troubleshoot and resolve computer problems	Post password on desk, tape to monitor, write on notes, hide under mouse pad, etc.
Examples of good passphrases, because they have no meaning: SpokenMeetStrains RevisionLobbySociety JudgesLiquidBelieve	Examples of bad passphrases, because they have meaning, or are commonly heard: WeThePeople ToBeOrNotToBe DeepDishPepperoniPizza LoudPipesSaveLives AthensTheaterDeLand
Examples of more good passphrases, because they have no meaning and contain symbols or numbers: #SubsetKingdomHours PromptRecordHinted5 CarpetAdobe@LeastBear	Use common keyboard sequences, such as qwerty00 or abc12345.
	Use phrases from movies and books, or common phrases.
	Use words that naturally go together and have meaning.
	Increment passwords by adding a sequential number on the end when changing it.
	Give, email, text, fax, or release passwords to anyone.

Information Technology Responsibilities

- Verify the identity of a User prior to providing assistance in resetting a password.
- Assist Users in resetting passwords when the User has forgotten their password or suspects their password(s) is compromised.
- Assist in adding or removing a User's Computing Resource security.

Direct Supervisor Responsibilities

- Document employee passwords when appropriate and store in a secured central storage area (e.g., metal lockbox, safe, etc.) for use in emergencies. Management should only collect passwords that cannot be reset by the system administrator. Most passwords used for centralized computing service can be reset by system administrators whereas local passwords created to protect specific documents cannot. For example, Information Technology can change a user’s email and file server passwords at management’s request, but Information Technology cannot change passwords set by users to protect specific Excel spreadsheets, Word documents or Access databases.

- Contact the Information Technology Support Desk to add or remove a User's Computing Resource security. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Reporting Incidents

Background

Computer related incidents impact the County's ability to serve the public. An incident may impact a single User, a front counter application, or an enterprise-wide application used by hundreds of County employees. Such incidents can be costly in terms of repair and lost productivity and often get reported in the media which diminishes public trust.

Examples of computer related incidents include but are not limited to computer hardware or software failure, network failure, application outage, virus/worm intrusion, network intrusion, server corruption, application failure, ransomware, or workstation failure.

Procedure

Incidents will be identified and reported promptly.

All incidents will be responded to with a priority that addresses a timely, effective, and orderly recovery with the appropriate use of resources. Status updates will be provided at regular intervals during recovery.

Standards

- County Computer related incidents will be reported to and tracked by the Information Technology Support Desk.
- Local Information Technology support within the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact the Information Technology Support Desk as the situation dictates.
- All incidents will be promptly reported to minimize security exposures and improve recovery times.
- The Information Technology Support Desk will notify the IT Security Officer and activate the appropriate Information Technology resources to deal with the situation.
- The IT Security Officer or designee will oversee resolution, file the appropriate incident report, and maintain a current log (electronic and paper) detailing all security related incidents.

Guidelines

User Responsibilities

- Identify computer related incidents or suspected incidents (i.e. applications failing to perform correctly, logon failure, network connections not functioning, unusual text or graphics displayed on the monitor, and other faulty computer services).

- Immediately report computer related incidents or suspected incidents to the Information Technology Support Desk. Do not assume someone else has called in the incident. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

- Read and review Information Technology postings on ENN. Take appropriate actions as indicated by these postings or as instructed by IT Support Staff. Contact the Information Technology Support Desk if further assistance is needed. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Information Technology Responsibilities

- Monitor systems, network, and services for abnormal behavior and failures.

- Activate recovery staff when incidents occur or are reported. Record incident in appropriate log(s).

- Appropriately inform/update department/division liaisons or designees of current incident(s) and recovery progress.

- Disconnect and shut down affected equipment or network connections, if necessary, to prevent further damage or exposure.

- Research and resolve incidents through diagnostic facilities and processes. This includes working with appropriate personnel to verify data have not been corrupted, manipulated, or destroyed.

- Post a User information bulletin on ENN or contact department/division liaison when an outage is expected to exceed one-half hour (30 minutes).

- Place a follow-up ENN information bulletin or contact department/division liaison when the service is restored.

- Notify the person(s) reporting the incident via phone, email, or ENN posting as to resolution.

Spam Email

Background

Spam email can result in huge losses of productivity. Based on 2018 Nucleus Research statistics, unfiltered spam would have cost the County over $712 for each of the 2200 email accounts, totaling 1.5 million dollars per year in lost time.

No anti-spam solution can block 100% of spam. However, the percentage that does get through is negligible. Spammers continue to adapt and find new ways to avoid detection by anti-spam solutions. The anti-spam vendors then update their solutions to block the new technique. Employees can expect to see fluctuations in the amount of spam that reaches their email accounts each month as anti-spam vendors struggle to keep pace with spammers.

In addition to blocking incoming spam, the County also checks for malware activity in incoming and outgoing emails. The virus definitions used to screen for malware are updated daily through both automatic and manual updates.

2018 Spam Statistics (per month)	
Average spam blocked by County	2,500,000 to 3,000,000
Average legitimate emails permitted through	200,000 to 250,000
Average number of incoming emails containing suspected viruses	50

Procedure

The County will use an anti-spam system to filter out as many spam messages as possible, such as “work at home” advertisements, chain letters, mortgage solicitations, profanity, fraud, phishing, and known sources of unwanted and non-business related email.

Standard

The Information Technology anti-spam system uses hardware and special software to block spam email from getting into User email accounts. The software attempts to keep the "bad" email out, while letting legitimate email in. The software uses a list of words, phrases, sender addresses, and web links to check email entering the County email system. Most legitimate email passes the check and is sent on for delivery in seconds. Occasionally, a legitimate email may be blocked due to the words or phrases contained in the message. Blocked emails will be maintained for fourteen days and will be sent forward to the intended receiver upon request. A small amount of spam is expected to get through the anti-spam solution.

This anti-spam solution protects County Users including Elections, Library Services, and Property Appraiser. The Sheriff's Office is responsible for spam management in the Sheriff’s Office email system.

Guidelines

User Responsibilities

- Do not participate in the creation, forwarding, and/or sending of spam (advertisements, solicitations, chain letters, etc.).

- Forward email containing inappropriate solicitations or spam to the Information Technology Support Desk. This allows Information Technology to forward the spam to the anti-spam vendor, who will update the anti-spam filters. Sheriff's Office employees should contact their local IT support instead of the Information Technology Support Desk.

- Provide your County email address only to trusted web sites, mailing lists, individuals or vendors.

- Use of your county email address should be restricted to county-related business. All non-work related emails (shopping, social networking, personal finance, etc.) should be completed using a personal email account on a personal device (Hotmail, Gmail etc.) and on personal time.

- When you no longer wish to receive mailings from a valid publisher use the "unsubscribe" function, generally located at the bottom of the email.

- Contact the Information Technology Support Desk when you suspect that a legitimate piece of mail has been blocked or have other email delivery problems. Sheriff's Office employees should contact their local IT support instead of the Information Technology Support Desk.

Information Technology Responsibilities

- Provide spam filtering of the County email system.

- Forward copies of spam that were not blocked by the anti-spam solution to the vendor. The vendor will update spam filters on an ongoing basis to block spam email.

- Forward copies of spam that perpetuates a fraud or scam to the Federal Trade Commission and the anti-spam vendor.

- Assist Users that suspect a legitimate email was blocked.

- Identify and release legitimate, quarantined email upon request.

Transferred, Separated, and Terminated Employees

Background

Department/division management approves access to County computer systems and data depending upon an employee's position and job responsibilities. When an employee changes positions or leaves County employment, the requirement to access information and computer systems also changes or ends. Similar to employees turning in keys, identification badges, and other job related tools when changing positions or leaving the County, an employee's access to computer systems and data must also be "turned in" promptly for reassignment or deletion. Dormant or out of date User accounts provide an opportunity for misuse of County computer systems while appearing to be legitimate.

Procedure

Access to Computing Resources must be restricted to authorized Users. Authorization to use Computing Resources will be limited to the User's need to fulfill job requirements. Department/division management is responsible for ensuring that security is appropriate when an employee's, contractor's, or vendor's position or responsibilities change.

Department/division management is responsible for revoking access to Computing Resources when an employee leaves County employment or a vendor or contractor is no longer doing business with the County. Department/division management is also responsible for determining if access to Computing Resources shall be suspended or revoked as a result of disciplinary action.

Accounts and passwords will be appropriately disabled on transfer or termination of employees, contractors, or vendors. Department/division management will take appropriate and timely steps to notify the security administrators (County, State, Federal, banking, etc.) of all systems the transferred, separated, or terminated employee accessed.

Standards

- Access to Computing Resources is restricted to authorized Users. The revocation of User access due to a disciplinary action including termination will take place prior to or together with the action.

- Requests for revocation of User access due to an employee's, contractor's, or vendor's separation from the County will be made prior to separation and normally effective no later than the end of the last day of employment, unless specifically extended by department/division management.

- Requests for modification of User access due to transfers or changes in responsibilities shall be made prior to the change and will normally be effective together with the action, unless specifically extended by department/division management.

Guidelines

Direct Supervisor Responsibilities

Inform the Information Technology Support Desk of the requirement to change or revoke User access of an employee, contractor, or vendor prior to the action. If the situation requires special handling, work with the IT Security Officer to implement the change. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Information Technology Responsibilities

Ensure that User privileges are revoked or revised when informed of employee, contractor, or vendor change of responsibilities, transfer, separation, or termination.

IT Security Officer Responsibilities

Work with department/division management or designee when requested in order to coordinate changes in User privileges of an employee, contractor, or vendor requiring special handling.

Human Resources Division Responsibilities

Provide the Information Technology Support Desk with a list of employees separated or terminated on a bi-weekly basis.

Vendor Access to Computing Resources

Background

County computers, software, applications, and data used to provide County services may require support, installation, or modification by outside vendors. Some departmental systems may be wholly or partially supported by outside vendors. These vendors will need onsite and/or remote access to the systems to provide this support. Information Technology will provide guidance and enforce Standards for providing access to outside vendors in a secure manner. The term "vendor" is meant broadly and includes prime contractors and their subcontractors.

Procedure

Vendors providing support or services to the County for Computing Resources or solutions must adhere to the County *Computing Security Procedures*. Managers within the responsible department/division will ensure that vendors are required to read, understand, sign, and follow the County *Computing Security Procedures* as if they were County employees. Prime contractors are responsible and accountable for ensuring their subcontractors fully adhere to the County *Computing Security Procedures*.

Vendor access to the County network and Computing Resources will be implemented in a controlled, secure, and monitored environment.

Standards

The County maintains a virtual private network (VPN) solution to provide remote access by vendors and employees. The VPN solution provides for authentication of the vendors, encryption of communication, and authorization of selected Computing Resources by logon. All connectivity will be arranged through a County contact.

County intervention will be required for a vendor to gain access to the network or Computing Resources (e.g., virtual escort, enabling a vendor VPN logon). The vendor will identify the length of time that access is needed.

Vendors will promptly notify the County that temporary VPN access is no longer needed when they complete services. Information Technology will disable the VPN account until it is needed again. Vendor VPN accounts will only be enabled for pre-determined periods of time authorized by the County.

Guidelines

Department/Division Responsibilities

- Contact the Information Technology Support Desk to request a vendor account for accessing or revoking access to County Computing Resources. Employees of the Sheriff's Office, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

- Educate vendors on the County *Computing Security Procedures* prior to vendor accessing computing resources. Obtain the signature of the vendor's authorized representative on the acknowledgement form from the County *Computing Security Procedures* indicating knowledge of and compliance with Procedures.

- Ensure vendors comply with practices and standards as specified in maintenance contracts and the County's *Computing Security Procedures*.

Information Technology Responsibilities

- Provide County portion of remote access solution for vendors.

- Enable and disable vendor remote access as required.

- Provide support for educating vendors in access practices and requirements as specified in maintenance contracts and the County's *Computing Security Procedures*.

- Remove vendor account upon notification from department/division liaison.

- Document and maintain an approved vendor access list.

- Ensure that vendors use County Approved Encryption Methods when accessing or storing County data that is required to be protected to meet regulatory compliance.

Vendor Responsibilities

- Use County Approved Encryption Methods when accessing or storing County data that is required to be protected to meet regulatory compliance.

- Provide notification to the County when employees associated with County projects and services leave employment or are reassigned.

- Limit access to County data to only those with a legitimate need to know.

- Comply with practices and standards as specified in maintenance contracts and the County's *Computing Security Procedures*.

Appendix A: Definition of Terms

Approved Encryption Methods

For any protected information encrypt data in transit and at rest using the following technology:

Data in Transit
Any FIPS 140-2 certified method and at least 128 bit strength.

Data at Rest
The same as above or a FIPS 197 certified method such as BitLocker for Windows 10 and at least 256 bit strength.

The passphrase used to unlock the cipher for any encrypted file shall meet the following requirements:

i. Be at least 10 characters.
ii. Not be a dictionary word.
iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
iv. Be changed when previously authorized personnel no longer require access.

CJI

Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following data types are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

CJI Authorized Personnel

An individual, or group of individuals including contracted services, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Computing Equipment

Includes but is not limited to workstations, laptops, mobile devices, and servers. Loosely defined as a general-purpose machine that processes data according to a set of instructions that are stored internally either temporarily or permanently.

Computing Resources

Computing Resources include, but are not limited to, all software, hardware, workstations, laptops, tablets, servers, applications, data, media, smartphones, and networks (LAN, WAN, WLAN) that belong to Volusia County, or are attached to the County network.

County

Volusia County

County Network

All voice, data, and video networks connected to devices directly configured or supported by Information Technology staff.

ENN

Employee News Network. The County's intranet web site.

ePHI

Electronic protected health information refers to any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

Guideline

Guidelines are steps taken in compliance with the Procedures, which include areas of responsibility.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is United States legislation that provides data privacy and security provisions for safeguarding medical information.

HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Information Technology

The Information Technology Division (ITD) of Business Services. There are some instances where another division or individual is responsible instead of ITD. Elections, Library Services, Property Appraiser, and Sheriff's Office have local department/division support staff for workstations and servers. These areas should substitute local department/division support for ITD, when workstations or servers are involved. ITD works in coordination with these local resources as the situation dictates.

LAN

Local Area Network. A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.

PII

Personally identifiable information. This is any data that could potentially identify a specific individual.

Procedure

A Procedure is a guiding principle established by senior management that an organization or project adopts to influence and determine decisions. A Procedure demonstrates commitment from senior management to certain behaviors. It states management's commitment to a program, describing a high-level philosophy and topical coverage. Information security Procedures are brief, technology and solution-independent documents.

Protected Health Information (PHI)

Protected Health Information is defined in 45 CFR 160.103, where "CFR" means "Code of Federal Regulations", and, as defined, is referenced in Section 13400 of Subtitle D ("Privacy") of the HITECH Act. Protected health information means individually identifiable health information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and, (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Standard

Standard represents a specific approach, solution, methodology, product, or protocol that must be adhered to for establishing uniformity. Standards are required to maintain consistency and to avoid variance where inappropriate. Standards may be geared toward the User or the technician. Information Technology Standards evolve in step with the progression of technology.

Trusted Sites

Trusted Sites are websites that you know and trust not to damage your computer or harvest information such as passwords and credit card numbers. Examples include Staples (https://eway.com) and Amazon (https://amazon.com).

User

User refers to anyone using County Computing Resources including direct employees of the County as well as consultants, vendors, contractors, and others performing on the behalf of the County.

WAN

A wide area network is a telecommunications network, usually used for connecting computers, that spans a wide geographical area. Unlike LANs, WANs typically do not link individual computers, but rather are used to link LANs.

WLAN

A wireless local area network is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection.

Appendix B: Publishing Procedures

1. Update ENN intranet home page.
2. Update IT ENN home page.
    a. Also publish supporting documents such as Smartphone_Reset_Guide.pdf, Anti_Virus_Guidelines.pdf, Jump_Drive_Procurement_Guidelines.pdf and others to Resources/Standards on the IT ENN page.
3. Send copy to Purchasing. This is used by vendors who need access to county systems.
4. Send copy to Human Resources. This is used during new employee orientation.
5. Reset the first-time login popup in Active Directory. This causes users to re-validate that they have read and accepted the document.

Computing Security Procedures Acknowledgement

This form is used to acknowledge receipt of, and compliance with the County *Computing Security Procedures*. Management shall have employees, contractors, and vendors read the Procedures and sign this acknowledgement when first employed and annually thereafter.

Complete the following steps:

1. Read *Computing Security Procedures*. Fill in requested information in the spaces provided below including signature and date.
2. Retain a copy of this page for your records.
3. Return this page to your direct supervisor for inclusion in the department/division's personnel records.
4. Vendors and contractors return this page to the County project manager for inclusion in the County project file.

Signature

By signing below, I agree to the following terms:

i. I have been provided access to and read a copy of the *Computing Security Procedures* and understand the same;
ii. I understand that any Computing Resource provided to me by the County or accessed by me may contain confidential information about Volusia County and its citizens or its vendors, and that this is and remains the property of the County at all times;
iii. I agree that I shall not copy, duplicate or distribute any software provided to me by Volusia County without appropriate authorization;
iv. I agree that I shall not copy, duplicate or disclose, or allow anyone else to copy or duplicate, sensitive information except as required as a part of my job here at Volusia County;
v. I agree that, if I leave Volusia County for any reason, I shall immediately return to the County the original and all copies of any and all data, software, computer materials, or computer equipment that I may have received from the County that is either in my possession or otherwise directly or indirectly under my control.
vi. I understand that it is a condition of employment to sign and abide by this document.
vii. I understand and agree that I shall not install any unauthorized software without Information Technology authorization.

Employee Signature	
Employee Name	
Employee ID	
Date	
Department	
Division	