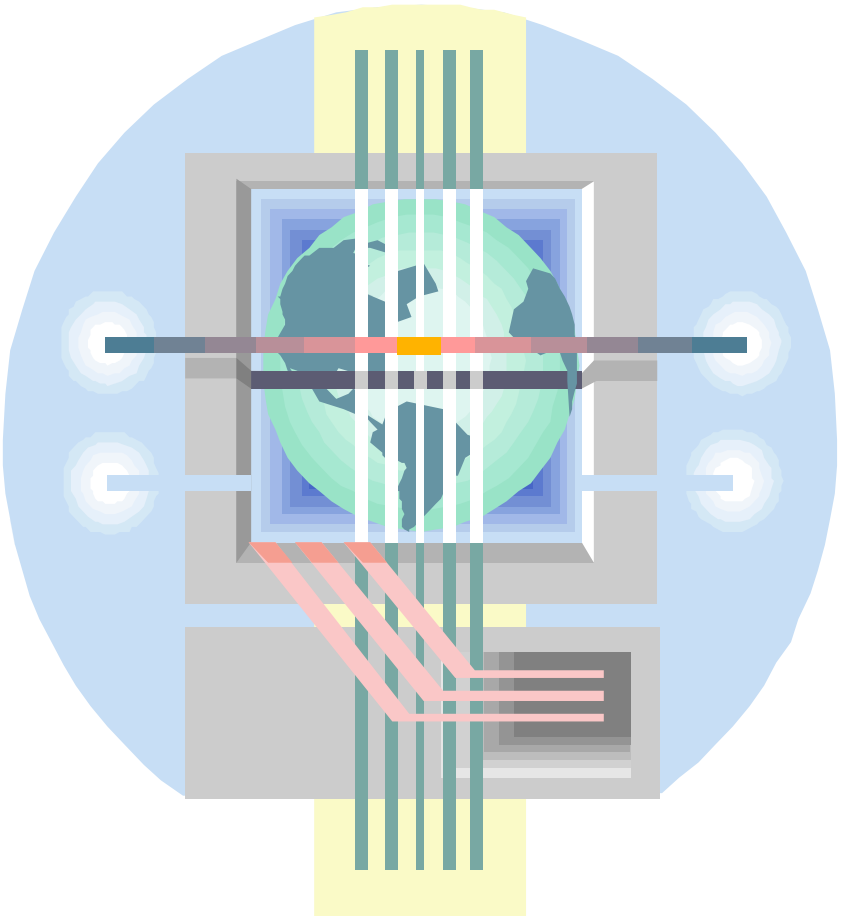
COMPUTING SECURITY PROCEDURES

Volusia County
FLORIDA



VOLUSIA COUNTY, FLORIDA

Updated: October 2011

TABLE OF CONTENTS

OBJECTIVES, SCOPE, AND COMPLIANCE 3

AVOIDING COMPUTER VIRUSES AND HOAXES..... 4

DISPOSAL OF COMPUTING EQUIPMENT AND MEDIA..... 7

EMPLOYEE REMOTE ACCESS 9

EQUIPMENT, DATA, AND MEDIA..... 11

INTERNET 14

NETWORK EQUIPMENT 16

PASSWORDS..... 18

REPORTING INCIDENTS..... 20

SPAM E-MAIL 22

TRANSFERRED, SEPARATED, AND TERMINATED EMPLOYEES..... 24

VENDOR ACCESS TO COMPUTING RESOURCES..... 26

APPENDIX A: DEFINITION OF TERMS 28

ACKNOWLEDGEMENT OF COMPUTING SECURITY PROCEDURES – SIGNATURE REQUIRED 30

Objectives, Scope, and Compliance

Objectives of Procedures

The primary objective of the *Computing Security Procedures* is to protect County of Volusia (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, 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 sub-contractors.

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

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).

Definition of Terms

Definitions are included in Appendix A: Definition of Terms

Avoiding Computer Viruses and Hoaxes

Background

Computer viruses, worms, spyware, and trojan horses are programs designed to make unauthorized changes to applications, files, e-mail, networks, and data. These programs can cause the destruction and/or corruption of County Computing Resources, compromise information, and can inhibit Users from completing work. Introducing a virus, worm, trojan horse, or other malicious programs 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 are e-mails or similar warnings of virus or worm outbreaks. Along with the warning are instructions to prevent infection. These instructions typically involve deleting files and forwarding the warning on to friends and relatives. If you delete these files your system will no longer function correctly and may not even be able to boot up.

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 as released by the anti-virus vendor.

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 as released by the anti-virus vendor.

Information Technology staff will post a notice to Users via ENN Hot News, e-mail, phone, or other notification processes for virus threats and known hoaxes that may impact the County.

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 servers, workstations, and laptops are initially set up to automatically download anti-virus updates from the anti-virus servers when they are posted.

Guidelines

User Responsibilities

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

- Report virus symptoms, anti-virus software warnings, and suspected hoaxes to the Information Technology Support Desk at 740-5222 (extension 5222). Do not forward the virus. Employees of the Sheriff, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

- Load data, 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 jump drive, CD, DVD, diskette, other electronic storage media, and the Internet. How-to instructions are available on Information Technology's ENN home page under the training section.

- Ensure that the anti-virus software is running on your workstation on a daily basis. How-to instructions are available on Information Technology's ENN home page under the training section.

- 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 and enabled on non-County equipment used on behalf of the County prior to connecting equipment to County equipment or utilizing County data.

- Contact the Information Technology Support Desk at 740-5222 (extension 5222) if further assistance is needed. Employees of the Sheriff, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Information Technology Responsibilities

- Install and maintain appropriate anti-virus protection software on all County Computing Equipment including but not limited to workstations, laptops, tablets, and servers. Local IT support within the Sheriff, Elections, Library Services, and Property Appraiser will install and maintain appropriate anti-virus protection software on all equipment under their control.

- Maintain anti-virus protection for the County e-mail system, including Elections, Library Services, and Property Appraiser, that automatically identifies and deletes infected e-mail or attachments. Local IT support within the Sheriff's Office is responsible for the Sheriff's e-mail anti-virus protection.

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

- Broadcast in a timely manner, information regarding widespread virus outbreaks or hoaxes likely to impact the County.

Disposal of Computing Equipment and Media

Background

County Computing Equipment and data storage media may contain software, applications, and data used to provide County services. If left on Computing Equipment or data storage media upon disposal, sensitive information such as social security numbers, credit card account numbers, or passwords may pose a security risk or expose personal information. Data storage media includes but is not limited to jump drives, diskettes, CDs, and disk drives in devices such as computers, copiers and scanners,

Procedure

County data, software, and applications are protected resources. They are not to be left on Computing Equipment and/or media at time of disposal.

Data storage media must be formatted and/or destroyed prior to disposal.
User data and profiles must be erased from data storage media prior to repurposing.

Standards

County data, software, and applications residing on County Computing Equipment will be erased prior to disposal using current best practices for the type of media.

Data storage media will be reformatted using software meeting Department of Defense standards and/or rendered non-usable by physical means. CDs, DVDs, floppy disks, and like type media will be shredded or broken into multiple pieces. Scraping away recording media with a sharp object is also an acceptable alternative. Hard disk drives, jump drives, memory cards, and like media will be shredded or crushed until the drive is inoperable.

County data, software, and applications on County Computing Equipment being repurposed will be erased and/or media reformatted depending upon the situation.

Guidelines

User Responsibilities

- Format or render non-usable by physical means all portable data storage media including but not limited to disk drives, jump drives, diskettes, CDs, and tape prior to repurposing or disposal.
- Contact the Information Technology Support Desk at 740-5222 (extension 5222) to arrange for a workstation analyst to destroy data on Computing Equipment prior to repurposing or disposal.
- Contact the Information Technology Support Desk at 740-5222 (extension 5222) if further assistance is needed. Employees of the Sheriff, Elections, Library Services, and

Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

Information Technology Responsibilities

- Format Computing Equipment disk drives prior to repurposing.
- Format, remove, and destroy all disk drives in County Computing Equipment prior to being sent out to surplus, auction, trash, or other valid disposal method.
- Destroy all data including software on leased County Equipment prior to release to lessor.
- Format or render non-usable by physical means all portable data storage media including but not limited to disk drives, jump drives, diskettes, CDs, and tape prior to disposal.

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 home PC or laptop, therefore employee owned home PCs are considered unmanaged or unsecured computers.

Each remote access account and access point to the County network increases the security risk. Management is asked to limit remote access requests to employees whose use will significantly benefit County operations. To limit security exposures, management is discouraged from providing remote access to employees for casual use.

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.

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 County Information Technology approval are a violation of this Procedure.

The County is not responsible for the configuration, repair, or diagnosis of non-County PCs, laptops, equipment, or software. Remote access from home PCs and employee owned laptops is discouraged to prevent security breaches.

Standard

Remote access to County e-mail does not require a User to have access to the County network. Access is provided via the Internet at **https://vcmail.vcgov.org**.

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

Guidelines

User Responsibilities

- Safeguard hardware or software that may be provided by the County.
- Provide personal Internet accounts, phone lines, cable connections, remote wiring, etc. required at home or outside of County premises.
- Install and maintain appropriate security software including, but not limited to anti-virus software, security patches, and automatic software updates.
- 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 home PC or an employee owned laptop.
- Ensure that remote access 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 password protected screen saver if workstation is left unattended while signed into remote access account.
- Contact the Information Technology Support Desk at 740-5222 (extension 5222) if further assistance is needed. Employees of the Sheriff, 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 at 740-5222 (extension 5222) 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 Users to only those applications required to perform their duties.
- Provide Users guidance in configuration, access, and utilization of remote access.
- Provide for the maintenance, diagnosis, and repair of County owned hardware and software.

- Quarterly, provide department/division liaison to Information Technology or his/her designee a listing of remote access accounts for verification that information is accurate. Disable accounts where appropriate.

Equipment, Data, and Media

Background

Computer hardware, software, and networks are the property of the County of Volusia 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, March 21, 2007. The policy is located at http://enn.co.volusia.fl.us/communityinfo/Communications%20Policy.pdf

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

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. 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.

Management retains the right to inspect any and all files, equipment, and logs created and/or stored on County owned computers or computers connected to the County networks.
It is the employee's or vendor's responsibility to suitably protect from loss or theft any data in their possession. Data encryption is required when removing laptops or electronic media from the County facilities if the data files contain sensitive or confidential information such as social security numbers or credit card numbers. The encryption can be accomplished using software such as TrueCrypt.

Installation of all computer software on County owned computers must be authorized by Information Technology.

Standards

Software installation on County owned computers 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 screen savers will be configured to activate after fifteen minutes of inactivity on a workstation or laptop computer.

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 jump drives, CDs, DVDs, diskettes or other media out of sight when not in use. If they contain highly sensitive or confidential data, they should be suitably secured. When warranted, encrypt the data. When in doubt, request Information Technology or department/division recommendation on encryption.

- Protect Computing Resources including desktops, laptops, jump drives, CDs, DVDs, diskettes and media from environmental hazards such as heat, direct sunlight, magnetic fields, food, smoke, liquids, humidity, and extreme heat or cold. Users who neglect this will be accountable for any loss or damage that may result.

- Contact Information Technology Support Desk at 740-5222 (extension 5222) for equipment recommendations and approval (i.e. laptops, PDAs, printers, GPS units, plotters).

- Contact Information Technology Support Desk at 740-5222 (extension 5222) 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. Load 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 workstation 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 workstation. Contact Information Technology Support Desk at 740-5222 (extension 5222) if screen saver does not activate on workstation after fifteen minutes of inactivity.

- Lock the password protected screen saver whenever workstation 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 to Information Technology Support Desk at 740-5222 (extension 5222) and direct supervisor. Employees of the Sheriff, 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 at 740-5222 (extension 5222) if further assistance is needed. Employees of the Sheriff, 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 workstations, laptops, and tablets. The screen saver will be set to come on after fifteen minutes of inactivity.

- Set up password protection on workstations, laptops, and tablets to be invoked at system start-up.

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

- Install workstations, laptops, and tablets with appropriate software security measures including, but not limited to anti-virus software, patches, automatic software updates, and passwords.

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

- Provide consultation on data encryption.

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 computer systems to unauthorized access and tampering. Industry statistics show that PCs connected to the Internet possess an increased likelihood of being infected with spyware programs and viruses. The malicious programs can result in data corruption or damage to computer systems. According to the 2010 CSI/FBI Computer Crime and Security Survey of over 350 information security practitioners, virus incidents were the most frequently occurring security issue.

Procedure

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

Standard

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

Guidelines

User Responsibilities

- Abide by the Volusia County Communications Policy, March 21, 2007 regarding Internet use. The policy is located at http://enn.co.volusia.fl.us/communityinfo/Communications%20Policy.pdf

- Ensure that any transactions involving sensitive information such as credit card numbers, 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 VeriSign protected sites or a similar security offering for transactions involving sensitive information such as credit card numbers, passwords, and social security numbers.

- Do not use instant messaging such as AOL Instant Messaging from a Volusia County Computing Resource.

- Check that the anti-virus software on your workstation 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 anti-virus 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 at 740-5222 (extension 5222) if further assistance is needed. Employees of the Sheriff, 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 desktops with Internet access unless directed not to by department/division management.

- Maintain Internet access servers.

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

- Block access to restricted sites and services as approved.

- Recover from Internet service failures in a timely manner.

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.

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 utilized within County facilities or connected to the County Network must be approved by Information Technology prior to installation.

Standards

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

Information Technology maintains Standards for equipment that is appropriate for use at remote sites, external networks, home offices, and mobile Users.

Guidelines

User Responsibilities

- Contact the Information Technology Support Desk at 740-5222 (extension 5222) 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 at 740-5222 (extension 5222) 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 at 740-5222 (extension 5222). This would include simply seeing a consumer wireless or wired network hub in the general work area.
- Monitor the activities of vendors, contractors, and employees to ensure that they comply with this Procedure.

- 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.

- Do not connect or otherwise allow wireless connections to any devices other than County authorized Access Points (APs).

- Contact the Information Technology Support Desk at 740-5222 (extension 5222) if further assistance is needed. Employees of the Sheriff, 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 prior to implementation.

- Install County networking and WLAN solutions.

- Perform wired and wireless network audits to identify any unauthorized access points on the network.

- Remove unauthorized access points on the network and report the removal to the department/division liaison, the Information Technology Director and the Information Technology Security Officer.

Passwords

Background

The confidentiality and integrity of data stored on County computer systems must be protected by passwords to ensure that only authorized employees, contractors, and vendors have access. This access shall be restricted to only those functions that are appropriate to each employee's, contractor's or vendor's duties.

Procedure

User passwords are the 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 employees, contractors, and vendors accessing County applications or Computing Resources.

Passwords will be changed anytime the employee, contractor, or vendor suspects that someone has unauthorized knowledge of their password.

Standards

Passwords will be a minimum of eight characters long and shall include at least one number and one letter. Longer and more complex passwords are recommended.

Passwords will not be composed of easily guessed content. 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 for a password. As an example, e-mail, 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. Where possible, passwords may be matched to simplify use.

Guidelines

User Responsibilities

- Passwords should not be written down and left in a work area no matter how well hidden.
- Record passwords only for emergency purposes as noted below.
- Ensure that access to Computing Resources can be gained in the event of the loss of an employee. This may require managers to keep employee passwords stored in a safe and secure holding area.

- Review and follow instructions for resetting network, GroupWise e-mail, and screen saver 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 at 740-5222 (extension 5222) immediately if a password is compromised	Use personal information like pets' and children's names, last names, birthdays, hobbies, addresses, nicknames, etc.
Choose a password that is easy to remember but hard to guess	Use same password as on your home PC or home e-mail account
Use 8 or more characters mixing letters and numbers	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
	Give or e-mail passwords to anyone. Exception: In some cases a workstation technician may need a user password. Users may enter it for them. If in doubt contact the Information Technology Support Desk at 740-5222 (extension 5222)
	Post password on desk, tape to display, write on notes, hide under mouse pad, etc.
	Use common keyboard sequences, such as qwerty00 or abc12345

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 suspects their password(s) are compromised or they have forgotten their password.
- 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 for use in the event of an emergency.
- Contact the Information Technology Support Desk at 740-5222 (extension 5222) to add or remove a User's Computing Resource security. Employees of the Sheriff, 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.

The Information Technology Support Desk receives incident reports and takes appropriate actions to provide for recovery. Timely recovery requires that all incidents be reported promptly.

Incidents with a cost per hour of downtime ranging from $1,000 to over $50,000 are widely reported in computer publications. A single server or network equipment outage can disable access to applications or services for hundreds of County employees.

Procedure

All incidents will be responded to with a priority that addresses a timely, effective, and orderly recovery with the appropriate use of resources.

Incidents will be identified and reported promptly. Actions will be taken to resolve incidents as quickly as possible. Status updates will be provided at regular intervals during recovery.

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, or workstation failure.

Standards

County Computer related incidents will be reported to and tracked by the Information Technology Support Desk.

Local IT support within the Sheriff, 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 activate the appropriate Information Technology resources to deal with the situation.

Guidelines

User Responsibilities

- Identify computer related incidents or suspected incidents (i.e. applications failing to perform correctly, logon failure, network connections not functioning, and other faulty computer services).
- Report any incidents involving computing services to the Information Technology Support Desk at 740-5222 (extension 5222). Employees of the Sheriff, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.
- Report incidents in a timely manner. Do not assume that someone else has called in the incident.
- Read and review Information Technology postings on ENN. Take appropriate actions as indicated by these postings.
- Contact the Information Technology Support Desk at 740-5222 (extension 5222) if further assistance is needed. Employees of the Sheriff, 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 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.
- Shut down affected equipment or network connections, if necessary, to prevent further damage or exposure.
- Research and resolve incidents through diagnostic facilities and processes.
- Post a User information bulletin on ENN or contact department/division liaison when an outage is expected to exceed one-half hour.
- 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, e-mail, or ENN posting as to resolution.

SPAM E-mail

Background

Information technology research firm Nucleus Research, Inc. estimates that U.S. companies suffer $712 worth of lost productivity on average annually per employee due to unwanted and inappropriate e-mail (SPAM). That equates to over $1,200,000 for the County's 1,700+ e-mail accounts.

In 2010, the County blocked on average 3,000,000 pieces of SPAM e-mail monthly and on average delivered 145,000 e-mails (4.6%) as legitimate. The anti-SPAM solution is not able to block 100% of SPAM. Spammers continue to adapt and find new ways to avoid detection by anti-SPAM solutions. Then the anti-SPAM vendors update their solutions to block the new technique. Employees can expect to see fluctuations in the amount of SPAM that reaches their e-mail accounts each month.

Procedure

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

Standard

Information Technology uses anti-SPAM hardware and software to block SPAM e-mail from getting into User e-mail accounts. The software attempts to keep the "bad" e-mail out, while letting legitimate e-mail in. The software uses a list of words, phrases, sender addresses, and web links to check e-mail entering the County e-mail system. Most legitimate e-mail passes the check and is sent on in seconds. Occasionally, a legitimate e-mail may be blocked due to the words or phrases contained in the message. Blocked e-mails 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 e-mail system.

Guidelines

User Responsibilities

- Do not create and/or send SPAM (advertisements, solicitations, chain letters, etc.)
- Forward e-mail containing inappropriate solicitations or SPAM to the Information Technology Support Desk at e-mail address IT_SupportDesk. 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 e-mail address only to trusted web sites, mailing lists, individuals or vendors.

- Contact the Information Technology Support Desk at 740-5222 (extension 5222) when you suspect that a legitimate piece of mail has been blocked or have other e-mail 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 e-mail system.

- Forward copies of SPAM that were not blocked by the anti-SPAM solution to the vendor. The vendor will update SPAM filers on an ongoing basis to block SPAM e-mail.

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

- Assist Users that suspect they have had legitimate e-mail blocked.

- Identify and release legitimate quarantined e-mail in a timely manner.

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, pagers, 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 should 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 should 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 at 740-5222 (extension 5222) of the requirement to change the User access of an employee, contractor, or vendor prior to the action. Employees of the Sheriff, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

- Inform the Information Technology Support Desk at 740-5222 (extension 5222) of the requirement to 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, 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.

Personnel 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.

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 employees.

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 Users, encryption of communication, and authorization of selected Computing Resources by logon.

County intervention will be required for a User to gain access to the network or Computing Resources (i.e., powering on a modem, a positive response on a server, enabling a vendor VPN logon). Users will identify the length of time that access is required.

Guidelines

User Responsibilities

- Contact the Information Technology Support Desk at 740-5222 (extension 5222) to request a vendor account for accessing County Computing Resources. Employees of the Sheriff, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.
- Enable and disable vendor onsite and remote access as required. This may require assistance from Information Technology.
- 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*.

- Notify Information Technology Support Desk at 740-5222 (extension 5222) if vendor has changed or vendor access should no longer be granted. Employees of the Sheriff, Elections, Library Services, and Property Appraiser should contact their local IT support instead of the Information Technology Support Desk.

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.

Appendix A: Definition of Terms

Computing Equipment: Includes but is not limited to workstations, laptops, tablets, 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, cellular computing devices, and networks (LAN, WAN, WLAN) that belong to the County of Volusia, or are attached to the County network.

County: The County of Volusia

County Network: Consists of all voice, data, and video networks connected to devices directly configured or supported by Information Technology staff.

ENN: (Employee News Network) The County's internal Intranet Web site used to provide employees with information and links to services.

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

Information Technology: The Information Technology Division of Finance and Administrative Services. There are some instances where another division or individual is responsible instead of ITD. Elections, Library Services, Property Appraiser, and Sheriff 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.

ITD: ITD is the acronym for the Information Technology Division of Financial and Administrative Services. There are some instances where another division or individual is responsible instead of ITD. Elections, Library Services, Property Appraiser, and Sheriff 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.

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.

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.

Acknowledgement of *Computing Security Procedures* – Signature Required

This form is used to acknowledge receipt of, and compliance with, the County of Volusia *Computing Security Procedures*. Management is advised to 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. Return this page to your direct supervisor for inclusion in the department/division's personnel records.
3. Retain a copy of this page for your records.

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 computers, software, and storage media provided to me by the County or accessed by me may contain confidential information about the County of Volusia 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 (except for backup purposes as part of my job here at the County of Volusia), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;

iv. I agree that, if I leave the County of Volusia 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.

v. I understand that it is a condition of employment to sign and abide by this document.

vi. I understand and agree that I shall not install any software without Information Technology authorization.

1. Employee (or vendor) signature: _____
2. Employee (or vendor) name: _____
3. Date: _____
4. Department/division (or vendor company): _____