CITY OF DELTONA
ADMINISTRATIVE POLICY AND PROCEDURE

EFFECTIVE DATE	POLICY NUMBER	PAGE NUMBER	SUPERSEDES POLICY
03-26-21	CW19-02	1 of 17	Date: 01-07-19

Subject: Establishment of a Computer and Network Usage and Security Policy

Approved by:

_____
John A. Peters III, P.E., Acting City Manager

_____
Date

PURPOSE

The purpose of this policy is to establish administrative direction, procedural requirements and technical guidance to ensure the appropriate protection and usage of City of Deltona resources of an Information Technology nature.

SCOPE

This policy applies to all who access City of Deltona computer networks or use City of Deltona resources. Throughout this policy, the word "user" will be used to collectively to refer to all such individuals. The policy also applies to all computer and data communication systems owned by or administered by City of Deltona or its partners.

POLICY

All information traveling over City of Deltona computer networks that has not been specifically identified as the property of other parties will be treated as though it is a City of Deltona asset. It is the policy of City of Deltona to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. In addition, it is the policy of City of Deltona to protect information belonging to third parties that have been entrusted to City of Deltona in a manner consistent with its sensitivity and in accordance with all applicable agreements.

RESPONSIBILITIES

The Information Technology department is responsible for establishing, maintaining, implementing, administering and interpreting organization-wide information systems security policies, standards, guidelines and procedures under the authority of the City Manager. While responsibility for information systems security on a day-to-day basis is every employee's duty, specific guidance, direction, and authority for information systems security is centralized for all of City of Deltona in the Information Technology department. This department will perform information systems risk assessments, prepare information systems security action plans, evaluate information security products and perform other activities necessary to assure a secure information systems environment.

The Network Administrator is responsible for coordinating investigations into any alleged computer or network security compromises, incidents or problems under the direction of the IT director. The Network Administrator and Network Analyst are responsible for establishing security guidelines for appropriate user privileges, coordinating the monitoring of access control logs, documenting and applying security practices to systems, network devices and applications under the direction of the IT director. IT Staff are responsible for acting as local information systems security coordinators to assist the Network Administrator in implementing security best practices. All City staff are responsible for reporting all suspicious computer and network-security-related activities to the Information Technology department via email or through notification to helpdesk. In the event that a system is managed or owned by an external party, the department manager of the group leasing the services ensures with the external party that the system adheres to City policies and standards.

Department Directors are responsible for ensuring that appropriate computer and communication system security measures are observed in their areas. In addition to allocating sufficient resources and staff time to meet the requirements of these policies, department directors are responsible for ensuring that all employee users are aware of City of Deltona policies related to computer, communication and system usage.

All users are responsible for complying with this and any and all other City of Deltona policies defining computer and network usage or security measures. Users also are responsible for bringing all known information security vulnerabilities and violations that they notice to the attention of the Information Technology department.

SYSTEM ACCESS CONTROL

End-User Passwords

The City of Deltona has an obligation to effectively protect the data entrusted to it by citizens, employees, and partners; and to ensure the continuity of its business functions supported by its IT assets and resources. Using passwords that are difficult to guess is key step toward effectively fulfilling that obligation. Computer users are provided a username and password by City of Deltona IT staff. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the City of Deltona's entire network. All City of Deltona employees (including contractors and vendors with access to City of Deltona systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The following requirements were established based on industry standard security frameworks:

- **Passwords for user-level accounts, must be changed at least every 90 days**
- ITSD recommends users set a reminder in their outlook calendar to reset their password after 60 days. Otherwise, the computer will prompt with a warning and finally force the user (after 90 days) to change the password after logging off and logging in
- Password length must be 8 characters
- Passwords must meet complexity requirements. This means a password needs to meet 3 of the following 4 criteria:
    - Contain uppercase English character (ex. A-Z)
    - Contain lowercase English character (ex. a-z)
    - Contain at least one number (ex. 0-9)
    - Contain special characters (ex.!, #, $, %)
- Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Passwords must NOT be inserted into email messages or other forms of electronic communication or electronic files
- Poor, weak passwords have the following characteristics, and should be avoided:
    - The password contains words " City of Deltona", "city", "deltona", or any derivation
    - The password is a common usage word such as:
        - Names of family, pets, friends, co-workers, fantasy characters, etc.
        - Computer terms and names, commands, sites, companies, hardware, software
        - Birthdays and other personal information such as addresses and phone numbers
        - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
        - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Passwords should never be written down or stored on-line.

- Do not use the same password for City of Deltona accounts as for other non-City of Deltona access (e.g., personal IS account, benefits, etc.)
- Do not share City of Deltona passwords with anyone, including other city staff.
- All passwords are to be treated as sensitive, confidential COD information.
- Do not use the "Remember Password" feature of applications (e.g., Chrome, Internet Explorer, Outlook, FortiClient)
- Do not store passwords in a file on ANY computer system (including phones, tablets or similar devices) without proper encryption
- It is against City of Deltona policy to SMS text a password to end users
- It is against City of Deltona policy to share your password with anyone. This may or may not include your supervisor, a friend or relative, a student or part-time worker or even a co-worker

- **ITSD does not know your password! This is a common misconception. Passwords are encrypted and not accessible to any ITSD staff member**
- ITSD can reset your password to one that follows the above rules; however, once you log in you will be immediately prompted to change it to another complex password that follows the above rules
- If you change your password, remember to change your password on your smartphone or tablet, otherwise you won't get email on your device!
- If someone demands a password, refer them to this document or have them call the City of Deltona ITSD to determine the validity of their request
- If an account or password is suspected to have been compromised, report the incident to the City of Deltona IT Department immediately and change all passwords as soon as possible
- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Please do not use either of these examples as passwords!
- Password cracking or guessing may be performed on a periodic or random basis by the City of Deltona IT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it

Password System Set-Up

All computers permanently or intermittently connected to City of Deltona local area networks must have password access controls. Multi-user systems (servers) should employ user IDs and passwords unique to each user, and user privilege restriction mechanisms with privileges based on an individual's need to know. Network-connected, single-user systems must employ hardware or software controls approved by Information Technology that prevent unauthorized access.

All vendor-supplied default fixed passwords must be changed before any computer or communications system is used in production. This policy applies to passwords associated with end-user user IDs and passwords associated with privileged user IDs.

Where systems software permits, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three unsuccessful attempts to enter a password, the involved user ID must be temporarily disabled for no less than 30 minutes. The VPN and Outlook Web Mail constant connections must have a time-out period of 30 minutes and should log out upon reaching this threshold.

Whenever system security has been compromised or if there is a reason to believe that it has been compromised, the

involved system administrator must immediately take measures to ensure that passwords are properly protected. This may involve resetting all user passwords and requiring users to change them prior to next system log on.

Whenever system security has been compromised, or if there is a reason to believe that it has been compromised, the involved system administrator must take measures to restore the system to secure operation. This may involve reloading a trusted version of the operating system and all security-related software from trusted storage media or original source-code disks/sites. The involved system then would be rebooted. All changes to user privileges taking effect since the time of suspected system compromise must be reviewed by the system administrator for unauthorized modifications.

Logon and Logoff Process

All users must be positively identified prior to being able to use any City of Deltona multi-user computer or communications system resources. Positive identification for internal City of Deltona networks involves a user ID and password, both of which are unique to an individual user.

The combination of a user ID and fixed password does not provide sufficient security for Internet or remote connections to City of Deltona systems or networks. Modems, wireless access points, routers, switches or other devices attached to network-connected workstations or devices located in City of Deltona offices are prohibited and must be approved by the Information Technology Department.

If there has been no activity on a computer terminal, workstation, or personal computer for a certain period of time, the system should automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. The recommended period of time is 30 minutes.

SYSTEM PRIVILEGES

Limiting System Access

The computer and communications system privileges of all users, systems, and independently- operating programs such as system agents, must be restricted based on the need to know. This means that privileges must not be extended unless a legitimate business-oriented need for such privileges exists.

Default user file permissions must not automatically permit anyone on the system to read, write, execute or delete a system file. Although users may reset permissions on a file-by-file basis, such permissive default file permissions are prohibited. Default file permissions granted to limited groups of people who have a genuine need to know are permitted.

City of Deltona computer and communications systems must restrict access to the computers that users can reach over City of Deltona networks. These restrictions can be implemented through routers, gateways, firewalls, wireless access points, and other network components. These restrictions must be used to, for example, control the ability of a user to log on to a certain computer then move from that computer to another.

Process for Granting System Privileges

Requests for new user IDs and changed privileges must be in documented in a helpdesk ticket to the Information Technology department approved by the user's department director before any Information Technology department staff fulfills these requests.

Non City of Deltona employees or partners may not be granted a user ID or be given privileges to use City of Deltona computers or networks. All user ids are unique and linked to an individual, it is against City of Deltona policy to create generic access accounts for multiple users to use.

Privileges granted to users who are not City of Deltona employees must be granted for periods of 90 days or less. As needed, users who are not City of Deltona employees must have their privileges reauthorized by the sponsoring department head every 90 days.

Special privileges, such as the default ability to write to the files of other users, must be restricted to those responsible for system administration. Configuration changes, operating system changes, and related activities that require system privileges must be performed by system administrators.

Third-party vendors must not be given Internet or remote privileges to City of Deltona computers or networks unless a documented legitimate business need exist and is approved by City management. These privileges must be enabled only for the time period required to accomplish the approved tasks, such as remote maintenance. If a perpetual or long-term connection is required, then the connection must be established by approved extended user authentication methods.

All users wishing to use City of Deltona internal networks or multi-user systems that are connected to City of Deltona internal networks signify their agreement to comply with all applicable policies by their logon to the city network. An exception to this policy may be made if there is a justified business need and permission is acquired from the City Manager.

Process for Revoking System Access

All user IDs should have the associated privileges revoked after a certain period of inactivity not exceeding 180 days.

If a computer or communication system access control subsystem is not functioning properly, it should default to denial of privileges to users. If access control subsystems are malfunctioning, the systems should remain unavailable until such time as the problem has been rectified.

Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the IT director. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of City of Deltona policy. Requests that City of Deltona security mechanisms be compromised must not be satisfied unless the Information Technology Director approves in advance or City of Deltona is compelled to comply by law. Short-cuts bypassing systems security measures, pranks, and practical jokes involving the compromise of systems security measures are absolutely prohibited.

The privileges granted to users, based on their role within the organization, should be reevaluated by their departments annually. In response to feedback from City management, directors, department managers, the Human Resources department, or the IT director, IT Staff must promptly revoke all privileges no longer needed by users.

Department heads/Directors must report all significant changes in employee duties or employment status promptly to the Information Technology department or system administrators (for non-IT managed systems) responsible for user IDs associated with the involved persons.

For all terminations, the Human Resources department must issue a notice of status change to the Information Technology department through a helpdesk ticket and all system administrators who might be responsible for a system on which the involved employee might have a user ID.

INTERNET & COMPUTER USAGE

Granting Access

Internet access must be approved on a case by case basis by the Department Director and the City Manager. Upon approval, the Information Technology department will provide the end user with Internet access from the City network or from City resources.

Responsibilities of Users

The City of Deltona disclaims any warranty as to the quality or accuracy of electronic information via the Internet. The City shall have no liability for any direct, indirect or consequential damages related to the information contained therein. The City does not guarantee privacy or confidentiality for the use of City Internet systems.

All City users are expected to use City systems and resources, including the Internet, in a responsible and courteous manner, consistent with the occupational, business, educational and informational purposes for which the resources are provided. City users must abide by the Internet Usage Policy. Violations may result in the loss of Internet privileges or disciplinary action as defined in the City's Personnel Policies and Standard Operating Procedures. Illegal activities may be subject to prosecution by the appropriate law enforcement authorities.

The Information Technology department monitors and controls access to the Internet. Once access is granted, the Internet offers access to many valuable local, national and international sources of information. However, be aware – as with printed publications, not all sources on the Internet provide accurate, complete or current information. A good information consumer considers the source and evaluates the validity of information found.

The Internet is a global entity with a highly diverse used population and information content; Users use it at their own risk. The City of Deltona has filters in place at the network level to protect against sites with lewd, violent, discriminatory and terrorist related content or malicious code. No filtering product is 100% effective and users are urged to monitor their activities and report sites that fit unsuitable criteria. In addition the filtering software may block access to sites with legitimate value. Users doing bona fide research may request that the filters be disabled during their session. Such requests will be kept confidential. The City of Deltona restricts access to questionable Internet sites to comply with the laws and attempts to protect users from information they may find offensive.

All Internet resources accessible through the City of Deltona are provided equally to all approved users. It is the Users obligation to use those resources properly. Users may not use the network to make unauthorized entry or hack into other computational, informational, or communication services or resources. Users may not invade the privacy of others or engage in any activity that is harassing, defamatory or threatening; or receive or display text or graphics which may reasonably be construed as obscene as defined by law. The City of Deltona reserves the right to terminate any computer session where such material is displayed. Disciplinary action may follow.

Users are warned that public access computers are not secure. The City of Deltona cannot assure the confidentiality of credit card or other personal information transmitted through City computers. Users are often warned through workstation

messages not to disclose personal information in any form on electronic communication.

The City's Internet systems may not be used for any purpose that violates U.S., state or local laws. Users must respect all copyright laws and licensing agreements pertaining to files and other resources obtained via the Internet. Users may not use any City Internet system for illegal or criminal purpose including but not limited to harassment, stalking, pornography or scams. Users may not display materials that by community standards are obscene. Any use of the City Internet for "moonlighting", job searches, soliciting for commercial ventures, religious or personal causes or outside organizations, or for other similar non-job related solicitations is strictly prohibited.

Copyrights

U.S. copyright law (Title 17, U.S. Code) prohibits the unauthorized reproduction or distribution of copyrighted materials, except as permitted by the principles of "fair use". Users may not copy or distribute electronic materials (including text, images, programs, data or files) without the explicit permission of the copyright holder. Any responsibility for and consequences of copyright infringement lies with the users; the City expressly disclaims any liability or responsibility resulting from such use.

Rules governing the use of City workstations

- The City does not allow the use of games or personal software on City systems
- Users must virus check all external media (USBCD's, DVD's) to be used in City computers
- The Information Technology department can assist you with scanning the disks and safely transferring data
- Users may not obstruct other people's work by tampering with any City workstation
- Users may not make any attempt to damage computer equipment or software
- Users may not make any attempt to alter software configurations
- Users may not make any attempt to degrade system performance
- Users may not use any City workstation for any illegal or criminal purpose
- Users may not violate copyright laws or software licensing agreements in their use of City workstations
- Users may not engage in any activity that is deliberately or maliciously offensive, libelous or slanderous
- Users may not install software on City workstations or copy software from a City workstation
- Users may not use City workstations to play games
- Users of any computer workstation other than the one assigned is not allowed unless the other user has granted you permission to use their assigned system
- City equipment may not be unplugged, moved, removed, or otherwise modified by any user other than the authorized Information Technology employee.
- Users may not attempt to reconfigure systems or software or in any way interfere with the system set-up

Social Media Policy

This policy applies to all employees who use *Social Media* (via either a City computer/City internet access or using a personal computer/personal internet access) who makes reference to, or reflect upon, the City in any form.

Rules governing the use of *Social Media* (using either a City computer/City internet access or using a personal computer/personal internet access)

A. Social media activities should not interfere with City work commitments and should not be done during scheduled City work time.
B. Personal blogs, if related in any form to the City, should have clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of the City. Be clear and write in first person. Make your writing clear that you are speaking for yourself and not on behalf of the City.
C. Information published on your blog(s), if related in any form to the City, should comply with the City's confidentiality and disclose of proprietary data and/or public records policies. This also applies to comments posted on other blogs, forums, and social networking sites if related in any form to the City.
D. Be respectful to the City, other employees, customers, partners, and citizens.
E. Your online presence reflects upon the City if related in any form to the City. Be aware that your actions, captured via images, posts, or comments, can reflect upon the City.
F. Do not reference or site City clients, partners, or customers without their express consent. In all cases, do not publish any information regarding a City client during the engagement.
G. Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.
H. City logos and trademarks may not be used without written consent.

EMAIL USAGE

Understanding

The City of Deltona employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Further, the information passing through or stored on City equipment can and will be monitored if deemed necessary by a Department Head or the City Manager. The City of Deltona maintains the right to monitor and review e-mail communications sent or received by users, as necessary; such communications should not be considered private or secure.

The City of Deltona Information Technology departments has software and systems in place to monitor and record all e-mail usage and reserves the rights to do so at any time . No employee should have any expectation of privacy as to his or her e-mail usage. Our managers and directors will review e-mail activity and analyze usage patterns and they may choose to publicize this data to assure that City e-mail resources are devoted to maintaining the highest levels of productivity. We reserve the right to inspect any and all files stored in private areas of City computer systems in order to assure compliance with this policy.

Access

Access to the City's E-mail resources will be granted upon approval of a Department Head for those employees who are using computer systems capable of running the e-mail program, unless specifically denied access by the Department Head, or City Manager.

Conduct

All users are responsible for conduction themselves in an ethical and lawful manner when using City e-mail systems.

When creating e-mail messages the City of Deltona management expects you to follow the same standards required in hard copy business communications for the City. All e-mail accounts maintained on City of Deltona management expects you to follow the same standards required in hard copy business communications for the City. Users must understand that e-mail access is for the purpose of increasing productivity and not for non-business activities. Users must also understand that any connection to e-mail offers an opportunity for non-authorized users to view or access City information. Therefore, it is important that all connections be secure, controlled, and monitored.

The City of Deltona email account should be used primarily for the City of Deltona business-related purposes; personal communication is permitted on a limited basis, but non-City of Deltona related commercial uses are prohibited.

Email Retention

Florida Statute §119.011.1 defines public records for e-mail as "any message made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency." Business related City of Deltona e-mails are subject to retention laws. If, in doubt about e-mail retention, check with the City Clerk's office for clarification

Email retention is based on content, if an email meets a retention requirement it is the responsibility of the end user and department to retain that email on a file server or file cabinet for the necessary retention period. Otherwise, emails are saved in accordance with City policy of 3 years in a City archival system.

A. Business related e-mail (correspondence, inter-department memoranda, personnel, fiscal and budget records) that comply with "public records" criteria must be retained in your personal folder on the network for a period of three years. Your personal folder should be reviewed periodically, and e-mails that are older than the three year requirement should be deleted
B. "Non-business" related e-mail may be deleted when the intended purpose has been accomplished, or anytime at the users discretion
C. Any questions regarding retention can be directed to the City Clerk's Office

Emails stored on a "PST file" or off of the mailbox are subjected to these same requirements.

Email Archival System usage is granted on a per user basis at the discretion of the department director. The default access is to an employee's own email. Any access beyond the default access is granted at the discretion of the City Clerk's department. All usage of the Email Archival System is audited. Emails are stored for a period of 3 years and removed based on the latest yearly quarter. Emails from Multi-function copiers are not stored.

Security

- All the City of Deltona data contained within an email message or an attachment must be secured according to the Data Protection Standard
- Users are prohibited from automatically forwarding the City of Deltona email to a third party email system; such as Gmail
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct the City of Deltona business, to create or memorialize any binding transactions, or to store or retain email on behalf of the City of Deltona. Such communications and transactions should be conducted through proper channels using the City of Deltona-approved documentation
- City of Deltona management and the Information Technology department staff, under direction of a manager, can monitor any employee's e-mail account for legitimate business reasons in accordance with this policy

Guidelines for Authorized Use

The City of Deltona's e-mail service is intended for business use that means we expect you to use your e-mail account for business related purposes, i.e., to communicate with customers and suppliers, to research relevant topics, and to obtain useful business information. These are examples of authorized actions regarding use of your City of Deltona's e-mail account. The following actions are intended to be by example only and are not intended to be extensive.

- Subscribing to distribution lists and other forms of e-mail subscription services related to your job function. If in doubt seek manager or director approval before signing up
- System passwords are your best defense against unauthorized use of your e-mail account
- Do not compromise your account by giving your password to others, displaying it in public view or leaving Outlook open for others to use
- Encryption of e-mail is not necessary for most situations, but confidential messages can be encrypted. If in doubt, consult with your manager or director about confidentiality issues
- Users must exercise caution in addressing messages so it reaches the appropriate recipient.
- Spelling and grammar should be checked by the e-mail program before sending the message
- Long term message retention is important for relevant business or legal purposes. All incoming e-mail is automatically scanned for viruses and copied to an e-mail repository before you receive it. Outgoing mail is stored in your Sent Mail file on the local hard drive of the system you are using. Before you delete outgoing mail it must be reviewed for compliance with the retention policies. Business and legal correspondence must be copied to the appropriate retention folder on the network before it is deleted from your hard drive. If you desire to keep less important messages, please move those e-mails to your allotted personal folder on the network. If in doubt, check with the City Clerk's office for retention issues. Check with The Information Technology department for file size and storage considerations
- If you're saving emails in a "pst file" please be aware these files should not be stored on a file server and will not be backed up by the IT department, these are considered duplicate emails
- Avoid sending e-mail with large distributions, i.e. City-wide or department-wide messages because large volume tasks will adversely affect computer and network performance. If you require a distribution of 25 people or more, contact The Information Technology department for assistance. Only employees authorized by the Human Resources department may send to the "All Users" group
- Email is not a file transfer solution. Large e-mail messages and/or large e-mail attachments can significantly slow system and network performance. Messages and attachments that exceed 20MB in size will be removed by the server and those e-mails will not be transmitted. To transmit large files the IT department can assist you with the usage of an FTP server or file sharing service; such as dropbox

ESTABLISHMENT OF ACCESS PATHS

Changes to City of Deltona internal networks include loading new software, changing network addresses, reconfiguring routers, and adding remote lines. With the exception of emergency situations, all changes to City of Deltona computer networks must use the Information Technology department change management procedures and be documented in a helpdesk request. In addition, the request for change must be approved in advance by the Information Technology Director except as delegated emergency changes to networks must be made by persons who are authorized by Information Technology. This process prevents unexpected changes from leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to employees, but also to vendor personnel.

Employees must not establish electronic bulletin boards, local area networks, FTP servers, web servers and modem connections to existing local area networks, illegal Peer-to-Peer sharing or other multi-user systems for communicating information without the specific approval of the IT director. New types of real-time connections between two or more in- house computer systems must not be established unless such approval is obtained.

Acquisition of technology services or relying on an external party for network or computing services is prohibited unless City of Deltona City management has identified the risks involved and has expressly accepted these and other risks associated with the proposal, and the service provider meets the security and technology requirements identified by the Information Technology department.

All City of Deltona computers that connect to an internal or external network must employ password-based access controls or an extended user authentication system. Multi-user systems should employ software that restricts access to the files of each user, logs the activities of each user, and has special privileges granted to a system administrator. Single-user systems should employ access control software approved by the Information Technology department that includes boot control and an automatic screen blanker that is invoked after a certain period of no input activity.

Remote maintenance ports for City of Deltona computer and communication systems must be disabled until the time they are needed by the vendor or Information Technology staff. These ports must be disabled immediately after use and all usage must be documented for auditing purposes.

Portable devices (smartphones, tablet computers, etc.) using Wi-Fi or commercial data networks should not be used for data transmissions containing confidential personal information, unless the connection is encrypted. Such links may be used for electronic communications as long as users understand that confidential personal information must not be transmitted using this technology.

COMPUTER VIRUSES, WORMS, AND TROJAN HORSES

All computers must maintain approved and current virus-screening software enabled. This software must be used to scan all software coming from third parties or other City of Deltona departments and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses.

Users are responsible for reporting any potential security threats as soon as it is detected, the involved user must immediately call the Information Technology department to assure that no further infection takes place and that any experts needed to eradicate the virus are promptly engaged.

City of Deltona computers and networks must not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software and other software from untrusted sources must not be used unless it has been subjected to a testing regimen approved by the Information Technology department.

PRIVACY

Messages, information, or data sent over City of Deltona computer and communications systems are the property of City of Deltona. Management reserves the right to examine all data stored in or transmitted by these systems. City of Deltona computer and communication systems are to be used for business purposes, users are to have no expectation of privacy

associated with the information they store in or send through these systems.

When providing computer-networking services, City of Deltona does not provide default message protection services such as encryption. No responsibility is assumed for the disclosure of information sent over City of Deltona networks, and no assurances are made about the privacy of information handled by City of Deltona internal networks. In those instances where session encryption or other special controls are required, it is the user's responsibility to ensure that adequate security precautions have been taken. Nothing in this paragraph must be construed to imply that City of Deltona policy does not support the controls dictated by agreements with third parties, such as organizations that have entrusted City of Deltona with confidential information.

LOGS AND OTHER SYSTEMS SECURITY TOOLS

Every multi-user computer or communications system must include sufficient automated tools to assist the system administrator in verifying a system's security status. These tools must include mechanisms for the recording, detection, and correction of commonly-encountered security problems.

Whenever cost justifiable, automated tools for handling common security problems must be used on City of Deltona computers and networks. For example, software that automatically checks personal computer software licenses through a local area network should be used on a regular basis.

To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical City of Deltona information must securely log all significant security relevant events. Examples of security relevant events include users switching user IDs during an online session, attempts to guess passwords, attempts to use privileges that have not been authorized, modifications to production application software, modifications to system software, changes to user privileges and changes to logging system configurations.

Logs containing computer or communications system security relevant events must be retained for at least 30 days. During this period, logs must be secured such that they cannot be modified, and such that only authorized persons can read them.

Certain information must be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information must be securely stored offline until such time as it is determined that City of Deltona will not pursue legal action or otherwise use the information. The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, and copies of all potentially involved files.

Although system administrators are not required to promptly load the most recent version of operating systems, they are required to promptly apply all security patches to the operating system that have been released by knowledgeable and trusted user groups, well-known systems security authorities, or the operating system vendor. Only those systems security tools supplied by these sources or by commercial software organizations may be used on City of Deltona computers and networks. Additionally, only vendor-supported versions of operating systems and applications should be used on production systems. This will generally require periodic upgrades to the current release or the most recent prior version.

HANDLING NETWORK SECURITY INFORMATION

Information about security measures for City of Deltona computer and communication systems is confidential and must not be released to people who are not authorized users of the involved systems unless the permission of the IT director has been obtained. Security related information is exempt from public record as per statue 281.301, 282.318(4)(c)(d)(f), 286.0113(1), 197.071(3)(a), 119.071(1)(f) and (3).

PHYSICAL SECURITY OF COMPUTER AND COMMUNICATIONS GEAR

All City of Deltona network equipment must be physically secured. Access to data centers, telephone wiring closets, network switching rooms, and other areas containing confidential information must be physically restricted.

All employees who must keep confidential City of Deltona information offsite in order to do their work must possess lockable furniture for the proper storage of this information. At the time of separation from City of Deltona, all confidential information must be returned immediately.

VIOLATIONS

Violations of the Internet and Computer Usage Policy will be reviewed on a case-by-case basis. If it is determined that a user has violated the usage policies, management will take immediate action. Depending upon the nature of the violation, such disciplinary action may result in reprimand, termination of employment or possible legal action as established in the City's Personnel Policies and Standard Operating Procedures.

Unlawful activities will be dealt with in a serious and appropriate manner by the responsible law enforcement agencies, which will be notified of any such activities brought to the attention of the Human Resources Department.

When any employees believe that a user has failed to comply with the Network and Computer usage policy, they will report the violation to a Department Head. All disciplinary actions are determined by the Human Resources department and the City Manager.

REQUESTING HELP FOR IT RELATED ISSUES OR QUESTIONS

The Information Technology department staff is available to assist in issues, areas of concern, or questions relating to areas assign as a responsibility of the Information Technology Department. To request help please open a helpdesk ticket by going to the website: http://intranet/helpdesk or by emailing helpdesk@deltonafl.gov. You can also call our helpdesk staff at x8809 or x8805.

The Information Technology department prioritizes issues based on impact, staff time, and at management discretion.

TERMS AND DEFINITIONS

Access control: A system to restrict the activities of users and processes based on the need to know.

Agents: A new type of software that performs special tasks on behalf of a user, such as searching multiple databases for designated information.

Algorithm: A mathematical process for performing a certain calculation. In the information security field, it is generally used to refer to the process for performing encryption.

Badge reader: A device that reads employee identity badges and interconnects with a physical access control system that may control locked doors.

Booting: The process of initializing a computer system from a turned-off or powered-down state.

Bridge: A device that interconnects networks or that otherwise permits networking circuits to be connected.

Compliance statement: A document used to obtain a promise from a computer user that such user will abide by system policies and procedures.

Confidential information: A sensitivity designation for information, the disclosure of which is expected to damage City of Deltona or its partners.

Critical information: Any information essential to City of Deltona business activities, the destruction, modification, or unavailability of which would cause serious disruption to City of Deltona business.

Cryptographic challenge and response: A process for identifying computer users involving the issuance of a random challenge to a remote workstation, which is then transformed using an encryption process and a response is returned to the connected computer system.

Default file permission: Access control file privileges, read, write, execute, and delete, granted to computer users without further involvement of either a security administrator or users.

Default password: An initial password issued when a new user ID is created, or an initial password provided by a computer vendor when hardware or software is delivered.

Dynamic password: A password that changes each time a user logs on to a computer system. Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

Encryption: A process involving data coding to achieve confidentiality, anonymity, time stamping, and other security objectives.

End User: An individual who employs computers to support City of Deltona business activities, who is acting as the source or destination of information flowing through a computer system.

Extended user authentication technique: Any of various processes used to bolster the user identification process typically achieved by user IDs and fixed passwords, such as hand-held tokens and dynamic passwords.

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have passed some security check, such as providing a password.

Front-end processor (FEP): A small computer used to handle communications interfacing for another computer.

Gateway: A computer system used to link networks that can restrict the flow of information and that employ some access control method.

Hand-held token: A commercial dynamic password system that employs a smart card to generate one-time passwords that are different for each session.

Information retention schedule: A formal listing of the types of information that must be retained for archival purposes and the time frames that these types of information must be kept.

Isolated computer: A computer that is not connected to a network or any other computer. For example, a stand-alone personal computer.

Logon banner: The initial message presented to a user when he or she makes connection with a computer.

Logon script: A set of stored commands that can log a user onto a computer automatically.

Master copies of software: Copies of software that are retained in an archive and that are not used for normal business activities.

Multi-user computer system: Any computer that can support more than one user simultaneously.

Password guessing attack: A computerized or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorized access.

Password reset: The assignment of a temporary password when a user forgets or loses his or her password.

Password-based access control: Software that relies on passwords as the primary mechanism to control system privileges.

Password: Any secret string of characters used to positively identify a computer user or process.

Positive identification: The process of definitively establishing the identity of a computer user.

Privilege: An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user ID: A user ID that has been granted the ability to perform special activities, such as shut down a multi-user system.

Router: A device that interconnects networks using different layers of the Open Systems Interconnection (OSI) Reference Model.

Screen blanker or screen saver: A computer program that automatically blanks the screen of a computer monitor or screen after a certain period of inactivity.

Security patch: A software program used to remedy a security or other problem, commonly applied to operating systems, database management systems, and other systems software.

Sensitive information: Any information, the disclosure of which could damage City of Deltona or its business associates.

Shared password: A password known by or used by more than one individual.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Special system privilege: Access system privileges permitting the involved user or process to perform activities that are not normally granted to other users.

Suspending a user ID: The process of revoking the privileges associated with a user ID.

System administrator: A designated individual who has special privileges on a multi-user computer system, and who looks after security and other administrative matters.

Terminal function keys: Special keys on a keyboard that can be defined to perform certain activities such as save a file.

User IDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Valuable information: Information of significant financial value to City of Deltona or another party.

Verify security status: The process by which controls are shown to be both properly installed and properly operating.

Virus screening software: Commercially-available software that searches for certain bit patterns or other evidence of computer virus infection.

SIGN BELOW TO ACKNOWLEDGE RECEIVING, READING AND AGREEING TO THE TERMS OF THE CITY OF DELTONA INTERNET AND COMPUTER USAGE POLICY. SEPARATE THIS PAGE FROM THE POLICY. KEEP THE POLICY AND RETURN THIS SIGNED PAGE TO YOUR HUMAN RESOURCES REPRESENTATIVE FOR PLACEMENT IN YOUR PERSONNEL FILE.

By signing this form, I acknowledge that I have received a copy of the City of Deltona's Internet & Computer Usage Policy and I agree to be bound by its terms and conditions.

_____ _____

Printed Name Signature

_____

Department/Job Title

_____

Date