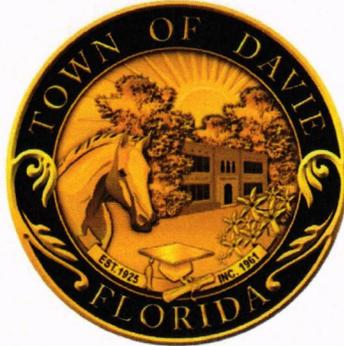


**TOWN OF DAVIE
HUMAN RESOURCES DEPARTMENT**



**TECHNOLOGY USE AND SECURITY POLICY
SOP #24-012**

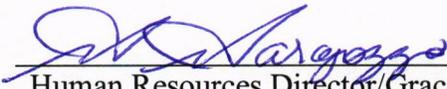
January 28, 2020

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

This operating procedure shall replace the Personnel Rules and Regulations and Policies enacted prior to the effective date of this Operating Procedure.

| Revision | Date | Responsible Department | Description of Change |
|-----------------|--------------------|-------------------------------|------------------------------|
| 1 | September 19, 2012 | Information Technology | Initial Release |
| 2 | July 29, 2015 | Information Technology | Revision |
| 3 | January 28, 2020 | Information Technology | Revision |

APPROVALS:


Human Resources Director/Grace Garagozzo

1/28/2020
Date


Town Administrator/Richard J. Lemack

01/29/2020
Date

1-1. POLICY.

This policy applies to all Internet access, electronic communications software and computer equipment attached to or used on the Town of Davie network system and applies to all Town of Davie owned software and hardware regardless of location or connectivity. This policy also implements systematic security guidelines to address the reduction of risks to electronic information resources. All individuals using the Town of Davie network system whether or not they are employees of the Town of Davie are required to adhere to this policy. The intent of this policy is to permit maximum freedom of use consistent with federal and state law, Town of Davie policy, and a productive working environment.

Use of Town of Davie computers and communication devices must comply with federal law, Florida law, and Town of Davie policies. Therefore, Town of Davie computers and communication devices may not be used for commercial, profit-making, or political purposes, or to disseminate unsolicited information regarding religious or political beliefs. With the rapidly changing nature of electronic media developing among users of external on-line services and the Internet, this policy cannot provide guidelines for every possible situation. Instead, it expresses the Town's philosophy and sets forth general principles for the use of Internet service and e-mail by all Town of Davie departments.

Information resources, including data, applications, systems, hardware, networks, and software, are valuable assets. These assets are at risk from potential threats such as employee error or other accidents, long-term system failures, natural disasters, and criminal or malicious action. Such events could result in damage to or loss of information resources, loss of data accuracy or integrity, or interruption of business. Information security guidelines address the reduction of risks to electronic information resources through adoption of preventive measures, procedures and controls designed to detect any errors or irregularities that occur.

This policy will also define standards, procedures, and restrictions for end users who have legitimate business requirements to use a Town of Davie issued mobile device that can access the organizations electronic resources. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook.
- Tablet computers such as iPads, Windows Surface Pro's, etc.
- Mobile/Cellular phones/Smartphones.
- Any mobile device capable of storing Town of Davie data and connecting to an unmanaged remote network.

The overall goal is to protect the confidentiality, integrity and availability of data that resides within the Town of Davie's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A

breach of this type could result in loss of information, damage to critical Town applications, financial loss, and damage to the Town of Davie's public image. Therefore, all users employing a mobile device connected to a managed or unmanaged network outside of the Town of Davie's direct control to backup, store, and otherwise access Town of Davie data of any type must adhere to the Town of Davie's defined processes for doing so.

Employees are responsible for complying with this policy. To ensure employees are aware of the provisions of this policy, they will be required to acknowledge acceptance of it before being allowed access to Town of Davie's electronic communications equipment. Department Directors are responsible for monitoring employee use and taking corrective and/or disciplinary action against employees in violation of this policy.

This policy applies to all Town of Davie employees, including full and part-time staff, elected officials, affiliates, contractors, interns, individuals and other agents who utilize Town of Davie owned or owned mobile devices to access, store, back up, support, relocate or access any Town of Davie resources / information. Such mobile and remote access to the Town's network resources / information is a privilege, not a right. Consequently, employment at the Town of Davie does not automatically guarantee the initial and ongoing ability to use these devices to gain access to the Town's networks and information.

1-2. SCOPE.

This policy applies to all Internet access, electronic communications software and computer equipment and mobile devices attached to or used on the Town of Davie network system and applies to all Town of Davie owned software and hardware regardless of location or connectivity. The policy applies to all individuals using the Town of Davie network system whether or not they are employees of the Town of Davie.

1-3. DEFINITIONS

E-mail: The electronic transfer of information typically in the form of electronic messages, memoranda and attached documents from a sender to one or more recipients via an intermediary telecommunication service.

Internet: A network of networks connecting computer systems throughout the world. In addition to e-mail capability, other applications such the World-Wide-Web (WWW or Web) are available on the Internet.

User: Any person who utilizes the Town's information systems, networks, computers, Internet, e-mail or electronic communication systems.

Chain letter: Any e-mail sent to one or more recipients that directs the recipient to forward the e-mail, so that its circulation increases exponentially.

Spam: Unsolicited bulk e-mail. Unsolicited means that the recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantially identical content.

1-4. PROCEDURE.

a. APPLICABLE LAWS

1. **Federal Copyright Law:** Many intellectual works are copyrighted. The owner of a copyright holds the exclusive right to reproduce and distribute the work. Most computer programs and manuals are copyrighted, and care must be taken to comply with copyright laws.
2. **State and Federal Trade Secret Laws:** Many intellectual works are protected under trade secret laws. Owners consider some programs and many manuals “trade secrets”. There are civil and criminal penalties associated with disclosing this information to anyone not authorized to use the material. Unless authorized in writing by the owner of the trade secret, you should not disclose any material that contains trade secret declarations to anyone outside Town of Davie government. **Software License Agreements:** Most computer software is licensed to a specific user or a group of specific users. The license agreement is very specific as to the rights that the user has to operate the program and make additional copies of the program. There are civil and criminal penalties associated with breaking a license agreement.

b. DEPARTMENT DIRECTORS AND SUPERVISORS RESPONSIBILITIES

1. Ensure that all personnel that use or have access to Town information systems, networks, computers, e-mail, Internet or electronic communication systems are aware of, and comply with this policy.
2. Create appropriate performance standards, controls and procedures that are designed to provide reasonable assurance that all users observe this policy.

c. INFORMATION TECHNOLOGY (IT) DIRECTOR RESPONSIBILITIES

1. Develop and maintain written standards and procedures necessary to ensure implementation of, and compliance with, this policy; and
2. Provide appropriate support and guidance to assist department directors, managers, supervisors and users fulfill their responsibilities under this policy.

d. INTELLECTUAL PROPERTY

The Town understands that during the course of a user’s tenure it may be necessary for said user to develop custom applications, scripts, templates and documents for the support

and benefit of the Town and its departments. All such applications, scripts, templates and documents developed by any Town user are the exclusive intellectual property of the Town. In no event shall any such computer program, data, documentation, listing, source code or object code be sold, licensed, released or loaned to individuals or entities outside the Town without the express approval of the IT Director and the Town Administrator. All items deemed as intellectual property will remain with the Town in the event the user leaves the Town for whatever reason.

e. INTERNET ACCESS

Access to the Internet is provided to users for the benefit of the Town, its residents and visitors. With it, users are able to access a variety of information resources around the world. Unfortunately, the Internet also contains considerable risk and inappropriate material. To ensure that all users are responsible and productive, and to protect the Town's interests, the following guidelines have been established for utilizing the Internet.

1. ACCEPTABLE USES

Users utilizing the Internet are representing the Town. Users are responsible for ensuring that the Internet is used in an effective, ethical and lawful manner. Examples of acceptable use include, but are not limited to:

- (i)** Obtaining Town related business and government information from commercial and government websites;
- (ii)** Accessing databases for information as needed by the Town;
- (iii)** Utilizing e-mail to conduct Town business;
- (iv)** To communicate with users, vendors or clients regarding matters within a user's assigned duties;
- (v)** To acquire information related to, or designed to facilitate the performance of regular assigned duties; and
- (vi)** To facilitate performance of any task or project in a manner approved by the user's supervisor.

2. UNACCEPTABLE USES

Users must not use the Internet for purposes that are illegal, unethical, harmful to the Town, or nonproductive. Examples of unacceptable use include, but are not limited to:

- (i)** Conducting a personal business utilizing computers or any other Town resources;
-

- (ii) Profit-making activities, such as but not limited to operating a business;
- (iii) Unlawful activities, including sending or receiving copyrighted or proprietary materials in violation of copyright laws or license agreements;
- (iv) Gambling and/or playing games;
- (v) Transmitting or accessing any non-job-related content that is offensive, harassing, sexually explicit or fraudulent. It is possible to connect to offensive websites accidentally in the course of legitimate research, and this should not cause alarm. Users are expected to close or back out of these windows immediately. Examples include, but are not limited to, pornography, gambling, and potentially offensive stories or jokes;
- (vi) Streaming transmissions, audio or video, unrelated to Town business. This includes, but is not limited to, radio and television webcasts unrelated to Town business. This does not include Town of Davie streaming webcasts viewed for Town purposes; and
- (vii) Intentionally utilizing Internet facilities to disable, impair or overload the performance of any computer system or network or to circumvent any system intended to protect the privacy or security of another user. That is, “hacking” in all forms, whether within the Town network or on the internet, is expressly forbidden, either from a user’s work computer or via access from a remote location, such as home.

f. E-MAIL USAGE

E-mails, and the electronic distribution of documents, are subject to the same laws, policies and practices that apply to other means of communication, such as telephone and paper documents and records. This includes, but is not limited to, copyright laws, software licensing, patent laws, record retention and proper business correspondence practices.

1. All communications are for professional reasons and do not interfere with their productivity or the productivity of others or in any way jeopardize the integrity or functionality of the system.
 2. They promptly read and respond, if necessary, to incoming messages.
 3. Any improper use of e-mail, including, but not limited to the following, is strictly prohibited:
 - (i) Sending any material in violation of Federal, State or County laws and/or Town policies;
-

- (ii) Sending harassing or otherwise threatening e-mails to a user or sending any message that may create a hostile work environment;
 - (iii) Sending any e-mail that discriminates against persons by virtue of any protected classification including, but not limited to, race, gender, nationality, religion, age, sexual orientation and so forth;
 - (iv) Sending inappropriate comments or jokes, cartoons or other communications that may be considered derogatory, obscene or offensive;
 - (v) Viewing pornography or sending photographs, videos, jokes or stories of a pornographic nature via e-mail;
 - (vi) Sending or receiving “spam,” chain letters or other types or communications that have the potential to interfere with the proper operation of the system;
 - (vii) Sending personal identification (including but not limited to name, address, e-mail address, telephone number, social security number, date of birth, mother’s maiden name, drivers license identification number, Florida Identification Card number, alien registration number, passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, credit or debit card expiration date, personal identification number or code assigned to the holder of a debit card by the issuer to permit electronic use of such card, other number or information that can be used to access a person’s financial resources, or medical records) for fraudulent purpose, financial benefit or harassment.
 - (viii) Sending credit or debit card numbers, credit or debit card expiration dates, personal identification numbers or codes assigned to the holder of a debit card by the issuer to permit electronic use of such card, or other numbers or information that can be used to access a person’s financial resources obtained while acting in their capacity or accessed as a result of their employment.
4. E-mails are not a secure form of communication. Users should avoid transmission of confidential information. If it is necessary to transmit confidential information for business purposes, users are required to take reasonable steps to ensure that the information remains confidential, is delivered to the intended recipient, that the intended recipient is authorized to receive such information, and that the intended use is legitimate. Data encryption is the only known reasonable method at this time.
5. The distribution of e-mails is difficult to control, and routing mistakes can easily occur. Copies of e-mails can be forwarded without the sender’s knowledge or permission to unintended recipients. Therefore, e-mails should be drafted and sent with at least the same level of care, professional judgment and discretion as paper memoranda or
-

documents.

6. Users are responsible for all e-mail messages originating from their e-mail address. The sender of e-mail messages and any attached documents must retain the primary responsibility for seeing that the communication is received by those intended.
7. Users shall not send mass e-mails without the prior written authorization of their Department Director.
8. Notwithstanding either the Town's right to retrieve and read any e-mail or any potential right of individual access to information that may be available under the Public Records Act, e-mail messages must be treated as confidential by other users and may be accessed only by the intended recipient. Users are not authorized to retrieve e-mail messages that are not sent to them unless the Department/Division Head provides user delegate access. Any exception to this requirement must receive prior approval from the IT Director and the Town Administrator.
9. Users should be cognizant that that e-mails can survive electronically for a very long time (even after deletion).
10. Access to Town e-mail shall be permanently revoked upon the user's termination or retirement. The Town shall not forward e-mail messages addressed to terminated or retired users.

g. INCIDENTAL AND OCCASIONAL PERSONAL USE

Incidental and occasional personal use of Town information systems, networks, computers, Internet, e-mail or electronic communication systems is permitted. However, personal use is prohibited if it:

1. Interferes with the user's productivity or work performance, or with any other user's productivity or work performance;
 2. Adversely affects the efficient operation of the Town's computer or electronic communication systems;
 3. Creates costs to the Town;
 4. Is unethical, unlawful, or inappropriate; or
 5. Violates any provision of this policy, or any other Town/departmental policy, regulation or guideline.
-

Users employing the Town's Internet, e-mail or electronic communication system for incidental and occasional personal use must present their communications in such a way as to be clear that the communication is personal and is not a communication of the Town.

h. DOWNLOADS

1. It is of critical importance from both a systems protection standpoint as well as to comply with the various laws in place protecting copyrights and proprietary data, that any software used that is licensed from a third party is to be used only in accordance with the license agreement. If anyone using software is uncertain whether the software may legally be used or duplicated for any purpose onto other Town computers, he or she should ask the IT Director.
2. To help prevent computer viruses from being transmitted through the system as well as to ensure compliance with the law, users are prohibited from downloading or installing software, including public domain software from the Internet, without the prior written approval of the IT Director. Any cost to repair damage incurred to any hardware, software or data resulting from the unapproved downloading/installation of software will be the responsibility of the user.
3. Downloading of games from the Internet or installing any on-line service to access the Internet on Town owned computers is prohibited.
4. Downloading of any executable files or programs that change the configuration of a user's system by anyone other than IT Department personnel is prohibited.
5. Software downloads from the Internet are not permitted unless it is work related and specifically authorized in writing by the IT Director.
6. Users may not utilize the Internet to download images or videos unless there is an express business-related use for the material.
7. Users must run a virus scan on all files received through the Internet. (*Procedure: Windows Explorer; Right Click, Highlight Drive; Click Scan*)

i. COPYRIGHTS

Users utilizing the Internet are not permitted to copy, transfer, rename, add or delete information or programs belonging to others without express written permission from the copyright owner. Failure to observe copyright or license agreements may result in disciplinary action by the Town and legal action by the copyright owner.

j. MONITORING

No user should have any expectation of privacy in any message, file, image or data created,

sent, retrieved or received by use of the Town's equipment and/or access. The Town has the right to monitor any and all aspects of its information systems, networks, computers, or electronic communication systems including but not limited to, sites, instant messages, chat groups, or news groups visited by users, material downloaded or uploaded by users and e-mails sent or received by users. Such monitoring may occur at any time, without notice and without the user's permission. Town-related computer files created on remote access personal computers must be made accessible upon request in Town standard formats.

All messages sent or retrieved over Town supplied information systems, networks, computers, e-mail, Internet or electronic communications systems may be regarded as public information. The Town reserves the right to access the contents of any messages sent over its facilities if the Town believes, in its sole judgment, that it has a business need to do so. All communications, including text and images, sent or retrieved over Town supplied information systems, networks, computers, e-mail, Internet or electronic communications systems can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

k. PUBLIC RECORDS

All users must comply with Florida's Public Records Act (Chapter 119 Florida Statutes) and State retention schedules for public records. The Public Records Law requires the retention and availability for copying of all materials, including e-mails, made or received by an agency in connection with official business, which are used to perpetuate, communicate or formalize knowledge. This also applies to mobile device for business related purposes as well (text messages, phone calls and pictures). Should you have a question about a particular request received in your department, contact the Town Clerk's Office as soon as possible.

l. BREACH OF SECURITY

The IT Director will adhere to the requirements of Florida Statutes Section 817.5681, and shall provide notice of any breach of the security of the system, following a determination of the breach, to any person whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, or subject to any measures necessary to determine the presence, nature and scope of the breach and restore the reasonable integrity of the system. Notification will be made no later than 45 days following the determination of the breach. For purposes of this section, the terms "breach" and "breach of the security of the system" mean unlawful and unauthorized acquisition of computerized data that materially compromise the security, confidentiality or integrity of personal information maintained by the Town. For purposes of this section, the term "personal information" means an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following

data elements when the data elements are not encrypted: (a) social security number; (b) driver's license number or Florida Identification Card number; and (c) account number, credit card number or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. For purposes of this section, the term "personal information" does not include publicly available information that is lawfully made available to the public from federal, state or local government records or widely distributed media.

m. COMPUTER VIRUSES

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of Town resources. It is important to know that:

1. Computer viruses are much easier to prevent than cure.
2. Defenses against computer viruses include protection against unauthorized access to computer systems, utilizing only trusted sources for data and programs, and maintaining anti-virus software.

(i) IT DEPARTMENT RESPONSIBILITIES

- (a) Install and maintain appropriate anti-virus software on all Town computers;
- (b) Respond to all virus attacks, destroy any virus detected and document each incident.

(ii) USER RESPONSIBILITIES

- (a) Users may not utilize the Town's Internet facilities to deliberately propagate any virus, worm, Trojan horse or trap-door program code;
 - (b) Users shall not load any external media such as diskettes, Compact Discs (CDs), USB flash drives or other data storage devices of unknown origin into a Town computer;
 - (c) Users shall not link personal mobile devices via wired or wireless connection to a Town computer;
 - (d) Users shall not tamper with the configuration of anti-virus software;
 - (e) Users shall scan all incoming files/data (diskettes, CDs, USB flash driver or other data storage devices) for viruses before they are read. (*Procedure: Windows Explorer; Right Click, Highlight Drive; Click Scan*);
-

- (f) Users must never open e-mail attachments that end with “.exe”, “.bat”, “.bas” or other known executable identifiers;
- (g) Any user who suspects that their workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the Help Desk at extension **1070**. This is one of the very few times that a normal shut down is discouraged.

n. ACCESS CODES AND PASSWORDS

The confidentiality and integrity of data stored on Town computer information systems and networks must be protected by access controls to ensure that only authorized users have access. This access shall be restricted to only those capabilities that are appropriate to each user's job duties.

1. INFORMATION TECHNOLOGY DEPARTMENT RESPONSIBILITIES

- (i) The IT Director shall be responsible for the administration of access controls to all networked Town computer systems. The IT Director will process user adds, deletes, and changes upon receipt of a written request from the end user's supervisor. Deletes, moves, adds or changes may be processed pursuant to an oral request prior to receipt of a written request;
- (ii) Accounts that remain inactive for an extended period may be deactivated, and then purged by the IT Director or designee.

2. USER RESPONSIBILITIES

- (i) Shall be responsible for all transactions that are made with their User ID and password;
 - (ii) Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained;
 - (iii) Shall change their passwords at least every 90 days. Users are encouraged to change their passwords greater frequency. For instance, if a user's birthday is February 10th, changing their password on the 10th of every month may be an easy habit to develop. (Note that the computer system will prompt users to change their passwords at least every 90 days);
 - (iv) Shall use complex passwords that cannot be easily guessed by others. Complexity of password: eight (8) character; upper case; lower case; special character and number; it is highly recommended that end users utilize fifteen (15) alphanumeric character passwords, possibly in the form of a passphrase.
-

- (v) Shall log out or log their workstation when leaving it unattended for any length of time;
- (vi) Must use their personal username and password;
- (vii) Shall store data and files on their designated file server. Because servers are backed up routinely, this protects against data loss.

3. SUPERVISOR RESPONSIBILITIES

Supervisors must notify the IT Director or designee immediately whenever a user leaves the Town, or transfers to another department/division, so their access can be revoked or changed. Involuntary terminations must be reported concurrent with, or prior to, termination.

4. HUMAN RESOURCES RESPONSIBILITIES

The Department of Human Resources will notify the IT Director monthly of user transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

o. PHYSICAL SECURITY

It is Town policy to protect computer hardware, software, data and documentation from misuse, theft, unauthorized access and environmental hazards.

1. USER RESPONSIBILITIES

- (i) Media (diskettes, CDs, USB flash drives, tapes or other data storage devices) should be stored out of sight when not in use. If they contain sensitive or confidential data, they must be stored in a locked secured location. Users are strongly encouraged to store such data on their designated file server;
 - (ii) Media should be kept away from environmental hazards such as heat, direct sunlight and magnetic fields;
 - (iii) Critical computer equipment, such as file servers and network equipment must be protected by an uninterrupted power supply (UPS). Other computer equipment must be protected, by a surge suppressor at minimum;
 - (iv) Computer and network hardware should not be exposed to environmental hazards such as food, smoke, liquids, high or low humidity, and extreme heat or cold. Where these hazards are unavoidable, appropriately hardened equipment
-

must be used;

- (v) Since the IT Director is responsible for all equipment installations, disconnections, modifications and relocations, users are not to perform these activities. This does not apply to portable computers for which an initial connection has been made by IT department personnel;
- (vi) Users shall not take shared portal equipment such as laptop computers off the premises without the informed consent of their immediate supervisor. Informed consent means that the supervisor knows what equipment is leaving, what data is on it and for what purpose it will be used;
- (vii) Users should exercise care to safeguard the valuable electronic equipment and related accessories assigned to them. Users who neglect this duty may be accountable for any consequent loss or damage. Reimbursement to the Town and disciplinary action can result;
- (viii) Users are reminded that existing policy concerning care and handling of Town property also applies to computer equipment.

p. SOFTWARE INSTALLATION

The goal of the IT Department is to provide stable technology solutions with optimum performance that appropriately address business needs. Implementation of these standards with regards to software titles that can be installed on Town owned computers is to ensure the provision of excellent service to all end users and Town wide departments.

The purpose of this software installation section is to address all relevant issues pertaining to appropriate software installation and deployment on the Town computing systems. This policy is a living document as it relates to the "Supported Software" section below and may be amended at any time. Any questions regarding should be directed to the IT Director.

1. **SUPPORTED SOFTWARE:** Contact IT personnel for a list of fully supported, standard baseline software installed on all Town-owned workstation computers.
 2. **NON-SUPPORTED SOFTWARE:** The IT Department expressly forbids installation of the following software:
 - (i) Privately owned software;
 - (ii) Internet downloads;
 - (iii) Pirated copies of any software titles;
-

- (iv) Any titles not listed in this policy unless expressly approved by IT personnel;
- (v) Any software not installed according to the procedures set out in this policy;
- (vi) Any Peer to Peer and/or messaging software applications (e.g. *Napster, Morpheus, KaZaa, Bearshare, AOL, P2P, I-Tunes, etc.*);
- (vii) Non-business related music files (e.g. *WAV, MP3, MIDI, etc.*) or video files (e.g. *MPEG, AVI, etc.*).

3. SOFTWARE REQUESTS

If you would like to have software installed on your system, approval must be obtained from the IT Department. This includes all software titles listed above, currently unlisted titles, and privately owned and licensed titles. The IT Department reserves the right to reject any software installation request for any reason.

Please fill out a copy of the Software Request Form located on the Intranet and return it to your department/division head for forwarding to the IT Department with an approved budget code.

4. SOFTWARE INSTALLATION

Software titles are to be installed on Town-owned equipment exclusively by IT Department personnel, or under their direct supervision.

All software installed on the Town systems (including all commercial and shareware products) must be used in compliance with all applicable licenses, notices, contracts and agreements. The IT Department reserves the right to uninstall any unapproved software from Town-owned equipment at any time.

5. PERIODIC AUDITS

The IT Department reserves the right to monitor software installation and usage on the Town's information systems, networks, computers, Internet or electronic communication systems. The IT Department will conduct periodic software metering audits to ensure compliance with this policy. Unannounced, random spot audits (*logical and physical*) may be conducted as well. During such audits, scanning and elimination of computer viruses and unauthorized files may also be performed. Other unsanctioned software may also be uninstalled at this time.

1-5. MOBILE DEVICES ACCEPTABLE USE.

As stated, the overall goal is to protect the confidentiality, integrity and availability of data that resides within the Town of Davie's technology infrastructure including Town owned

cell phones and personal phones. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical Town applications, financial loss, and damage to the Town of Davie's public image. Therefore, all users employing a mobile device connected to a managed or unmanaged network outside of the Town of Davie's direct control to backup, store, and otherwise access Town of Davie data of any type must adhere to the Town of Davie's defined processes for doing so.

This section of the policy addresses a range of threats:

| Threat | Description |
|-----------------|--|
| Loss | Devices used to transfer, or transport work files could be lost or stolen. |
| Theft | Sensitive District data is deliberately stolen and sold by an employee. |
| Copyright | Software copied onto a mobile device could violate licensing. |
| Malware | Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device. |
| Compliance Loss | Malware or theft of financial and/or personal and confidential information / data could expose the college to the risk of non-compliance with various identity theft and privacy laws. |

The addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of Davie IT. Unauthorized use of mobile devices to back up, store, and otherwise access any Town of Davie related information / data is strictly forbidden.

a. Use of Mobile Devices

It is the responsibility of any Town employee (*full time, part time, affiliate, contractor, intern, individual, etc.*) or elected official of the Town of Davie who uses a mobile device to access Davie information resources to ensure that all security protocols normally used in the management of data within the corporate network environment are also applied here. It is imperative that any mobile device that is used to conduct Town of Davie business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. It is also important to note that the Town

of Davie does not allow for the connectivity of any personal mobile devices on its enterprise network. Based on this, the following rules must be observed:

b. Access Control

1. Davie IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to the Town of Davie infrastructure. Davie IT will engage in such action if it feels such equipment is being used in such a way that puts the Town of Davie's systems, applications, data and staff at risk.
2. Prior to initial use on the Town of Davie network or related infrastructure, **all mobile devices must be procured by and registered with Davie IT**. Davie IT will maintain a list of approved mobile devices and related software applications and utilities as needed. Devices that are not on this list may not be connected to the Town's infrastructure. Although Davie IT currently allows only listed devices to be connected to the Town's infrastructure, it reserves the right to update this list in the future.

All mobile devices attempting to connect to the Town of Davie network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by the Davie IT department. Devices that have not been previously approved by Davie IT, do not comply with the Town's IT security policies, or represent any threat to the Davie network or data will **not** be allowed to connect. Only Town issued mobile laptop or desktop computers will be allowed to access the Town's network remotely using an approved Virtual Private Network (VPN) connection that employs the use of MFA (Multi-Factor Authentication).

c. Security

3. **Employees** using mobile devices and related software for network and data access **will**, without exception, use secure data management procedures. All mobile devices must be protected by a **strong password**. See section **1-4 (n) - Access Codes and Passwords**" of this policy for additional details. **Employees agree to never disclose or share their passwords with anyone**.
 4. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, employing strong passwords, encryption (*as required*), and physical control of such devices whenever they contain Town of Davie data.
 5. Davie IT will manage all security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation would be deemed as an intrusion
-

attempt and will be dealt with in accordance with the Town of Davie's approved Human Resources processes.

6. Employees, contractors, full time or part time personnel, elected officials, temporary staff and interns will follow all Davie IT-sanctioned data removal procedures to permanently erase Town of Davie specific data from such devices once their use is no longer required.
7. In the event of a lost or stolen mobile device, it is incumbent on the user to report this to Davie IT and their immediate supervisor or manager immediately. The device will be remotely wiped (wherever possible) of all data and locked to prevent access by anyone other than Davie IT personnel. If the device is recovered, it can be submitted to Davie IT for possible re-provisioning via the Town approved mobile device management solution.
8. Employees, contractors, full time or part time personnel, elected officials, temporary staff and interns **will make no modifications of any kind** to Town of Davie-owned and installed hardware or software without the approval of the Town of Davie's Department of Information Technology. This includes, but is not limited to, any reconfiguration of the mobile device.
9. The Department of Information Technology reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of any and all end users to transfer data to and from specific resources on the Town of Davie network.

d. Organizational Protocol

10. The Department of Information Technology can and will establish audit trails and these will be accessed and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to the Town of Davie's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Davie IT's highest priority.

1-6. POLICY NON-COMPLIANCE

Failure to comply with this policy or any of its associated policies mentioned herein may, at the full discretion of the Town of Davie, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.
