	POLICY AND PROCEDURE
	SUBJECT: COMPUTER, TECHNOLOGY, AND INTERNET USAGE POLICY

DATE: OCTOBER 20, 2014 **NUMBER: FN-14-003**

I. PURPOSE

The purpose of this Policy is to establish guidelines for the use of City of Riviera Beach ("City") city-owned computers (desktops, laptops, netbooks, tablets, smartphones, etc.), peripheral hardware and information technology systems; the use of network resources and services, Internet and intranet (sometimes collectively referred to as information technology); provide guidelines for expected behavior; and provide safeguards for the City's Information Technology Division (IT) resources. This Policy requires that computer and technology Users maintain respect for the privacy of protected information at all times. A cooperative effort from every User is necessary to prevent misuse, eliminate the risk of liability to the City, and promote efficient utilization of IT resources and services. E-mail is addressed under Policy Number FN-14-002.

II. POLICY

The City is committed to providing an environment that encourages the use of computers, technology and electronic information as essential tools to support and advance the goals and objectives of the City. These resources are for official use by elected officials, City employees, and other authorized Users to meet the daily operational and business requirements of departments and agencies and to carry out their individual job duties. It is the responsibility of each User to ensure the technology is used for business purposes and in a manner that does not compromise confidentiality or other sensitive information.

It is the policy of the City to ensure that computers, software, and peripheral computer and technology equipment are properly used and maintained. **Users should have no expectation of personal privacy protection when using City-owned IT and related services.**

III. SCOPE

This policy applies to all elected officials, City employees, and other authorized Users whether full-time, part-time, intern, vendor, temporary, contract, volunteers or otherwise.

Violations of this policy shall be reviewed on a case-by-case basis. Employees are advised that violations of this policy are subject to progressive discipline as outlined in the City's Policy and Procedures manual and the Policy for Discipline and Control. Discipline for such violations may include having restricted or revoked access, written warning, suspension, or termination.

IV. DEFINITIONS

For the purpose of this policy, the following definitions apply:

A. Chain Mail – Unauthorized non-government or NON-business related email sent to large groups, the City's Microsoft Outlook Global Address List, or to unspecific destination addresses that suggest that the receiver should further disseminate the message.

B. Computer – Includes any desktop computer, laptop (notebook) computer, netbook computer, tablets or any other related computing device (e.g., smartphone, etc.) purchased and/or issued by the City.

C. Computer theft – Includes theft of computer and technology services, intellectual property such as copyrighted material, and any other property.

D. Computer trespass – Unauthorized use of computing devices to receive, delete or alter data or interfere with others' usage.

E. Copyright – The right granted by law to an author, publisher, or distributor, for exclusive production, sale, or distribution of specific computer and technology software or a software application.

F. Database – A collection of data or information organized in such a manner that a computer program can quickly search and retrieve desired pieces of data. A database is like an electronic filing system. Traditional databases are organized by fields, records and files. A field is a single piece of information; a record is a set of fields; and a file is a collection of records.

G. Electronic Mail (Email) – Information created or received on an electronic mail system including any text messages, instant messages, and computer files transmitted over a communications network. This includes any attachments, such as word processing documents, spreadsheets, presentations, graphical images and multi-media content. Email also includes messages sent from one person to one or more individuals or groups (including mailing list addresses) via electronic media usually over an internal or external network. For purposes of this policy, vehicle-to-vehicle chat messaging used by the Police and Fire departments is included in the definition of Email.

H. Firewall – A part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.

I. Freeware/Shareware – Freeware is copyrighted computer software that is made available to computer Users free of charge for an unlimited time. Shareware is a copyrighted software that is offered on a "try it before you buy it" basis.

J. Hacking – Gaining or trying to gain unauthorized access to systems and databases either internal or external to City of Riviera Beach information technology systems or networks for the purpose of viewing, stealing, or corrupting data.

K. Hardware – The physical components of a computer system such as the motherboard, power supply, central processing unit (CPU), random access memory (RAM), secondary storage, plug-in adapter cards, internal removable media devices (e.g., CD, DVD, floppy disk, USB flash drive, tape drive, etc.), input and output devices, and peripherals. Hardware may also refer to other information technology system components or subcomponents.

L. Information Technology Systems – A group of interacting, interrelated and interdependent hardware, software, services and supporting infrastructure to store, manage and deliver information using voice, data and video. Examples are as follows: Computer and network systems (wired and wireless), Mesh and radio systems, Telephone systems and Voice response systems.

M. Internet – A global system of interconnected computer networks that use the standard Internet Protocol suite (TCP/IP) to serve billions of Users worldwide. It is a network of networks that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by a broad array of electronic and optical networking technologies. The Internet carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web and the infrastructure to support email.

N. Intranet – A private network designed for information sharing within an organization. It provides such services as document and/or software distribution, access to databases, and training. Intranet is so-called because it usually employs applications associated with the Internet, such as web pages, web browsers, File Transfer Protocol (FTP) sites, Email, newsgroups, mailing lists and is only accessible to those within the organization.

O. Message Definitions

1. Transitory Messages – Transitory messages do not set policy, establish guidelines, procedures, certify a transaction or become a receipt. Transitory messages are those records created for the purpose of informal communication of information and can be compared to a telephone conversation, written telephone messages, "post-it" notes, or verbal communications in a hallway. They are not designated for the perpetuation or formalization of knowledge.

2. Non-Transitory Messages – Non-transitory messages are those records which document or set official policies, actions, decisions, or transactions and are for the perpetuation or formalization of knowledge.

P. Network - A group of computers and associated devices that are connected by communications facilities for the purpose of sharing information and resources. A network can involve permanent connections such as cables, or temporary connections made through telephone or other communication links.

Q. Password – A security measure used to restrict access to a particular computer, technology, software or network system. A password is a unique string of characters that an authorized User enters as a method of identification. The system compares the password against a stored list of authorized passwords and Users. If the password is legitimate, the system allows the User access at whatever level of security has been approved for the individual owner of the password.

R. Peripheral Equipment – A device attached to a host computer that expands its capabilities, such as a printer, scanner, external data storage device (disk drive, tape drive, USB flash drive, etc.), docking station, microphone, speakers, camera, webcam, aircard, modem, and any other hardware that is connected to computing equipment.

S. Public Records – Public records are communications created or received in the transaction of official business and retained as evidence of official policies, actions, decisions, or transactions.

T. Record – A record includes all books, papers, maps, photographs, machine readable materials, or other documentary materials regardless of physical form or characteristics, made or received by the City in connection with the transaction of public business and preserved or appropriate for preservation as evidence of the organization, its functions, policies, decisions, procedures, operations or other activities because of the informational value of data in them. A record may be a something you can see, touch or feel or an electronic version.

U. Software – Digitally stored data such as a computer program and/or a set of instructions written in a specific language that commands the computer to perform various operations on data contained in the program or supplied by the User. Software includes the following: Platform software (firmware, device drivers, operating systems and graphical User interfaces); Application software (office productivity suites, business software, databases, educational software, computer games, etc.); Software tools & utilities to diagnose, repair or enhance computer operations; and User-written software (software that Users create such as special purpose programs, websites, web pages, intranet and software that Users modify such as existing software applications like spreadsheets, word processing documents, databases and email filters).

V. Software License – A written agreement by the software publisher and agreed upon by the software User, stating how the software may be used, the number of copies which may be made, how many Users may use the software at any one time, and any other requirement the software publisher wishes to be part of the agreement.

W. Users – Individuals authorized to use computers (desktops, laptops, netbooks and tablets), technology equipment, software, Email, the Internet and intranet as part of their assigned official duties.

X. User ID – The User ID by which an individual User is identified to a computer, technology equipment, software or network system. During the logon process, the User must enter his/her individually assigned User ID and password to gain access

Y. Virus/Malware – A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses/malware can also replicate themselves. All computer viruses/malware are man-made. A simple virus/malware that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus/malware is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus/malware is one capable of transmitting itself across networks and bypassing security systems. It can corrupt or destroy data stored on your computer and the network.

Z. Wireless – a term used to describe telecommunications in which electromagnetic waves carry the signal instead of wired media. Wireless refers to numerous forms of non-wired transmission such as AM/FM radios, cell phones, and wireless local area networks (LANs) and wide area networks (WANs). There are various techniques that are used to provide the transmission including cellular, microwave, Mesh, satellite and spread spectrum.

V. COMPUTER & TECHNOLOGY HARDWARE

A. Acquisition. In an effort to maintain consistency and stability in the City's information technology systems, IT will review all requests for Information Technology based hardware, software and maintenance prior to purchase or acquisition. The Information Technology Manager, or designee, will determine if the hardware or software is appropriate and compatible with the City's systems. Hardware, software and maintenance purchases will not be approved without the signature of the Information Technology Manager, or designee.

B. Installation. Installation of information technology hardware and software will be coordinated with the IT Staff and vendor, if applicable.

C. Users may be assigned computing and technology equipment for their use, but they are merely custodians of that equipment. The equipment remains the property of the City.

D. Equipment Moves. In order to ensure the safety of the City's equipment and proper connections, Users shall not move any equipment without the involvement and/or approval of IT Staff. In the event that a department needs to move computer equipment, the IT Staff shall be given sufficient advance notice.

E. Removal of Equipment from City Property. No equipment shall be removed, returned or exchanged without the prior approval of IT. If computing equipment is needed for home use, the User's request must be approved by the Department Director and IT. The Director must notify IT in writing about the change in location by providing IT with the custodian's name, the make, model and serial number of the equipment, and the date the equipment was taken home.

F. Users shall not attempt to change the configuration or setup of any City computing equipment. This is the sole responsibility of IT

G. Equipment Damage Prevention. Users are encouraged to follow the guidelines below to prevent damage to equipment:

1. Beverage containers and food should not be placed near computers, keyboards, mice, peripherals and technology equipment.

2. Eating and/or drinking near computer and technology equipment, especially keyboards, should not occur.

3. Anything that could fall or spill and ultimately damage the computer systems or hardware should not be located above or near any computers, peripherals or technology equipment.

H. Service and Repair. If a User's equipment needs to be repaired or serviced, the User must notify IT via a Track-It work order. IT staff will evaluate the equipment to determine if it should be fixed or replaced. Users are not authorized to place calls to vendors for equipment repair unless they have prior approval from the IT Staff.

I. Unless approved IT, Users are prohibited from connecting personal equipment and hardware devices (not City-owned) to the City's computing and technology equipment and network including, but not limited to, keyboards, mice, printers, scanners, cameras, hubs, switches, routers, bridges, gateways, wireless devices, etc. All hardware must be owned/leased by the City of Riviera Beach. The use of non-City-owned computing and technology equipment to connect to the City of Riviera Beach's network is **STRICTLY PROHIBITED**.

VI. COMPUTER & TECHNOLOGY SOFTWARE

A. Software Purchases. All software purchases for use on any City-owned computing and technology equipment must be pre-approved by the Information Technology Manager, or designee, for validity and compatibility.

B. The City has a Webmaster, therefore any request to create or change department web pages, or program interfaces to software applications must be entered as a Track-It work order and approved by IT

C. City software, for which the City has purchased a license, contains a license identifier linked to the City of Riviera Beach and shall not be used by any other person or entity.

D. Copyrighted software purchased by the City is considered proprietary in nature and shall not be reproduced or released to persons or groups not employed by the City for any reason. Software and programs developed by the City will be subject to the rules and regulations contained in Public Access Laws.

E. For the City's purposes, illegal or unauthorized software is defined as any software that has **NOT** been approved by the City's Information Technology Manager or designee and/or any software for which the City has **NOT** purchased or acquired a license.

F. Copying of City software is **STRICTLY PROHIBITED**. Absolutely no software shall be downloaded from the Internet, copied from the network to a DVD/CD-ROM, USB drive or any other media or system, or copied from one media to another either in the City or at home without previous written and specific permission from the Information Technology Manager or designee.

G. Copying of unauthorized software to the network or to any computer and technology equipment hard drives or media is not allowed. Absolutely **NO** unauthorized software shall be installed on any City system.

H. Copying of public domain software (i.e., Freeware/Shareware executables, etc.) to the network or to any computing and technology equipment hard drives is not permitted. Absolutely **NO** freeware/shareware software shall be installed on any City system unless approved and installed by IT

I. No personally owned software is authorized on the City's computing and technology equipment. All software must be legally owned and licensed by the City of Riviera Beach.

J. Any software that may be unique to a department's specific function within the City and may only need to be installed on a few computing devices within a department must still be pre-approved in writing by the City's Information Technology Manager or designee.

K. Software which is created or modified by a User for City-authorized projects or tasks becomes the sole property of the City.

L. The U.S. Congress has passed laws regarding software piracy, which is the unlawful copying of software. These laws carry very strict penalties and software piracy is now considered a felony, punishable by up to 5 years in prison and a fine up to $250,000.

M. Software Spot-Checking

1. At the direction of the City Manager, designated IT staff shall have the authority to audit, without notice, any computing or technology equipment in the City for unauthorized use and unauthorized software installations.

2. Any unauthorized software shall be removed immediately by IT staff or designee, who shall also file a report detailing the specific location of the incident, the type of software installed, and any damages that may have resulted from the unauthorized installation. The report shall be sent to the User's Department Director, with a copy to the City Manager.

3. IT staff is authorized to remove illegal and unauthorized software discovered while resolving computing and technology service requests or conducting physical asset inventories.

N. Unless authorized by IT to do so, Users may not run software that searches for means of obtaining unauthorized access, such as port scans, automatic login attempts, password crackers, and the like, whether or not they actually make unauthorized access after finding a way to do so on the City's network or on any City-owned computing or technology equipment.

O. Use of encryption software on any City computing device is prohibited without first obtaining written permission from the Information Technology Manager, and the encryption key shall be provided to IT for safe keeping.

VII. SECURITY

Authorized Users. City Users with assigned User IDs and passwords are the ONLY persons authorized to use City computing and technology equipment and network resources. No person is permitted to use any City computing and technology equipment or network resources without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use of any of the City's computing and technology equipment or network resources and services.

A. Unauthorized Usage. City Users are prohibited from using the City's computing and technology equipment, network, Internet and intranet systems for illegal purposes, unauthorized charitable endeavors, private business activities, or entertainment purposes. Users are reminded that the use of department resources, including electronic communications should never be used inappropriately nor shall the use create the appearance of impropriety.

B. Computer Security

1. To avoid security breaches, Users should log off and/or secure any computing and

technology equipment that has access to the City's network, email system, Internet or sensitive information whenever they leave their work areas. In addition, Users should make sure that they have password-protected screensavers on their computing devices that become activated after 10 minutes of inactivity.

2. During any logged-in period, Users of the City's computer system shall be responsible for all activity that occurs on that computer.

3. Users shall not allow unauthorized Users to access any file or database without the written permission of their Department Director.

4. Users shall not allow any other User to access computing and technology equipment or networks with their Username and password.

5. Each User must logon to use computing and technology equipment with his or her unique username (User ID) and password.

6. Users shall log off their computing and technology equipment or network and power down their devices at the end of every workday.

7. Users shall not attempt to circumvent or subvert any City-implemented system security measures.

8. Users shall not create Ad Hoc networks using wired or wireless network bridges, hubs, routers, wireless access points, wireless network interface cards, or any other network connection or device to access the City's network.

C. Password Security

1. Passwords are to be known only to the assigned User and shall **NOT** be shared.

2. Passwords should be memorized. They should not be stored in data files, taped to work stations or under keyboards, or programmed on function keys.

3. Passwords should be changed every 90 days.

4. Compromised passwords should be changed immediately.

D. Security Breaches.

IT must be notified immediately when:

1. A computer, laptop or technology equipment is lost or stolen. The User shall file a police report to document the incident and provide a copy to the Department Director, Information Technology Manager and Finance Fixed Assets Accountant.

2. Sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.

3. Unauthorized use of information technology systems has taken place, or is suspected of taking place.

4. Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen or disclosed.

E. Virus and Malware Control

1. Virus/malware detection. Viruses can cause substantial damage to computer systems and they can spread from one computer to another across the network. Antivirus software is installed and active on all servers, desktop computers and laptops.

2. The City has an antivirus server that distributes virus detection updates daily to each desktop networked computer and server for protection against viruses and malware infections. However, laptops must be updated manually. Users must schedule maintenance and antivirus/malware updates quarterly via the Track-It work order system.

3. Users should understand that their home computers and laptops might contain viruses/malware. Therefore, Users are discouraged from using media to transfer data from their work computers to their home computers and vice versa.

4. IT systems are in place to protect Internet and email traffic from virus/malware and spam. However, since antivirus/malware systems are not 100% effective, Users must take additional precautions when browsing or entering information on the Internet, and reading email containing attachments or website links.

   a. Email Security - All Email and attachments coming into the City's Exchange (Email) server are scanned for spam and virus/malware. This software also blocks certain types of files (.com, .exe, .bat, etc.).

      If a User is expecting but has not received a work-related email, the email may have been blocked by the City's email security filter. Contact IT via Track-It work order to unblock it.

   b. Web Security – All Internet websites requests are scanned for virus/malware and inappropriate content. If a User is blocked while attempting to visit a work-related website, the User should contact the Department Director who may approve the request and submit a Track-It work order asking IT staff to unblock the website. If the website appears to contain inappropriate content,

IT will forward the request to the City Manager or designee for review and appropriate action.

5. Computer viruses/malware spread quickly and must be eradicated as soon as possible to limit serious damage to computers and data. Accordingly, all Users must report a computer virus/malware to the IT Division as soon as it is noticed.

6. Unusual system behavior such as missing files, frequent system crashes, misrouted messages, etc. may indicate a computer virus/malware infection and IT shall be notified immediately.

VIII. EMAIL SYSTEM

Email is defined as all technologies used to transfer messages, including Email, instant messaging (e.g., Windows Messenger), and peer-to-peer file exchange. Email is a tool for business communications. City Users have a responsibility to use this resource in an efficient, effective, ethical and lawful manner. The City uses Microsoft Exchange and Microsoft Outlook for its email system.

Please review the City of Riviera Beach E-Mail Policy document.

IX. INTERNET USAGE

The City provides Internet access to City Users. They shall maintain a diligent and professional working environment when accessing the Internet. Internet access can provide a significant business benefit for the City, however there are legal, security, and productivity issues related to how the Internet should be used. The following guidelines are provided to Users:

A. Permitted Use

1. Users shall use the Internet for work-related purposes only. Examples of and work-related purposes include, but are not limited to the following:

   a. Job-related professional communication between other Users within the department or other City or government agencies.
   b. Accessing technical and other information which has relevance to the department.
   c. Maintaining professional and career development activities as approved by the Department Director.

2. The Internet shall be used in a manner that does not adversely affect system resources.

3. The use of the Internet shall not disrupt the operation of City business, nor cause Users to neglect or be inattentive to their duties.

4. Internet Users shall observe copyright restrictions of any document, image, or sound file.

B. Prohibited Use:

1. Use of technology resources for the purpose of personal financial gain or any commercial activity.

2. Use of technology resources for illegal or illicit activities.

3. Use of technology resources for viewing pornography or obscene materials of any kind, unless related to an active investigation or other official City business which has been authorized by the City Manager and/or Chief of Police.

4. Sending or receiving of copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

5. Vandalism including, but not limited to the uploading/downloading or creation of computer viruses/malware, or the attempt to destroy, harm or modify data of another User.

6. Use of City-owned computing equipment for placing any wager, bet or non-City work related bid.

7. Transfer of large volumes of data or numerous files that require excessive disk storage.

8. Use of City-owned computing equipment for playing online (Internet) computer games with or against other online player(s).

9. Use of City-owned computing equipment for playing online music, online videos, or other high-bandwidth applications for entertainment purposes.

10. Use of City-owned computing equipment for accessing inappropriate or unprofessional message boards, blogs or chat rooms, unless related to an active investigation which has been authorized by the City Manager and/or Chief of Police.

11. Entering a City business phone number on any non-City business related website which may cause recurring service charges to the City's monthly telephone bill.

C. Internet Spot-Checking

1. The City reserves the right to monitor any and all aspects of its computer,

technology and electronic communication systems, including, but not limited to, sites visited by Users on the Internet and reviewing material downloaded from or uploaded to the Internet by Users. Users should have no expectation of privacy with regard to Internet communications. The City may block access to certain websites for which access is deemed to be in conflict with City policy. Such monitoring may be conducted by designated IT staff without prior notice.

2. Illegal or improper activity shall be reported by IT to the Department Director in which the incident occurred and/or the City Manager's office.

X. PERSONAL USE OF COMPUTERS

A. The primary purpose of the City's computer system is to conduct City business.

B. Similar to telephone use, Users may occasionally send or receive personal Email, or access the Internet for personal reasons while at work. However, Users must use extreme care when doing so. Such instances of personal use shall be greatly limited, both in frequency and duration, and should not interfere with the performance of work duties and responsibilities or tax City resources.

XI. LAPTOP/TABLET USAGE

A. The primary purpose of the City's laptop and tablet computers is to provide Users with the ability to do computer-related work while away from their workplace. Authorized Users may also remotely access City applications, home directories and other network resources, as well as the Internet and Email to conduct City business. Many of these laptop computers are equipped with wireless aircards. Many of these tablet computers are equipped with SIM cards for Internet use.

B. Users who are assigned laptop and tablet computers, related documentation and accessories, whether on a permanent or temporary basis, shall be solely responsible for the care and safeguarding of their assigned laptop computers, the software therein, and accessories.

C. Distribution and Assignment

1. Permanently Assigned Units. When necessary, individual Users may be permanently assigned a laptop or tablet computer for their sole use. Except for laptops or tablets assigned within the Police Department, IT assigns laptops or tablets to authorized Users. In the Police Department, the Police Chief or designee will assign laptops or tablets to Police staff. The Police Chief or designee must provide IT with a written description, including User, make, model, serial number and date of assignment for each laptop or tablet.

2. Temporary Assigned Units. From time-to-time, Users may require the ability to utilize a laptop or tablet on a temporary basis for department approved City-related business. It shall be the responsibility of the User to contact IT in a timely manner to request the use of a laptop or tablet, and indicate the approximate length of time the laptop or tablet will be required and any specific software needs and access. IT will make every attempt to meet the User's needs if a laptop or tablet is available.

D. Laptop and tablet computer Users shall abide by the following guidelines:

1. All laptops or tablets that are to be utilized in vehicles shall be mounted in a docking station and should be outside of the 'airbag' zone to prevent injury to the User if the airbags were to deploy.

2. Users shall ensure the laptop or tablet is secured in its mount and the mount is locked into position while the vehicle is in motion.

3. Users shall not operate or manipulate the laptop or tablet while the vehicle is in motion if it interferes with the safe operation of the vehicle.

4. Users shall log off each time the laptop or tablet is left unattended, or secure the equipment from unauthorized access.

5. Users shall not alter, modify, tamper or delete any programs or program configurations on the laptop or tablet computer. This is the sole responsibility of the IT Division.

6. Users shall not install, or allow the installation of additional software onto the laptop or tablet computer or alter or modify configurations or setups.

7. Users may not password-protect, encrypt or hide any files on the laptop or tablet computer without providing IT with the password or encryption key.

8. Users are permitted to only use City-owned laptops or tablet for work-related tasks/duties.

9. Users shall not allow access to their laptop or tablet to anyone who is not authorized by the City of Riviera Beach.

10. Users shall not allow access to software programs by unauthorized personnel.

11. Users shall at no time use a City laptop or tablet to facilitate illegal or immoral activities.

12. Upon request, Users shall make their laptops or tablets available for inspection by supervisors and IT Staff.

13. Users shall schedule their laptops or tablets for quarterly maintenance and antivirus/malware updates via Track-It work orders.

14. Users shall not create Ad Hoc networks using wireless routers, wireless network interface cards or any other network connections or devices to access the City's network.

15. **Laptop Users must abide by the policies related to a desktop computer.**

E. Repairs

1. Users shall report problems or malfunctions with laptops to the IT Division via Track-It work orders.

2. Users shall ensure that the laptop assigned to them is not damaged or abused. This includes protecting it from liquids, rough handling or anything else that could cause damage.

F. If a laptop is damaged, lost, or stolen, the User should notify their supervisor, in writing, documenting the extent of damage and/or how the laptop was lost or stolen. In the case of stolen equipment, the User shall file a police report to document the incident and provide a copy to the Department Director, Information Systems Manager, and Finance Fixed Assets Accountant.

XII. COMMUNICATIONS

A. FCIC/NCIC Communications.

1. Many of the laptop computers assigned to police personnel, as well as the E911 Communications Center computer systems are set up to interface with the Florida Crime Information Center (FCIC) as well as the National Crime Information Center (NCIC).

2. Police department Users should be aware that access to FCIC/NCIC is regulated by Florida State Statutes as well as the Florida Department of Law Enforcement (FDLE).

3. Use of information in the system is strictly limited to law enforcement personnel and for law enforcement purposes only, and may not be disseminated to any person for any other purpose.

4. Use of the FCIC/NCIC networks is restricted to only those personnel who have been trained and are currently certified by FDLE.

5. Those personnel who have not received FDLE training are responsible for notifying the Police Department Communications Supervisor of their status and requesting appropriate training.

B. Unit-to-Unit Communications.

1. Some laptop computers are equipped with aircards which allow them to communicate vehicle-to-vehicle.

2. Police and Fire department Users should be aware that these are standard cellular communications which are regulated by the FCC and this City policy.

3. All communications via laptop computers and the VisionMobile software application are also logged in the Message Switch server. These records are subject to disclosure under public records laws and Users shall restrict all such communications to official business.

C. Law Enforcement Databases and Networks

1. The Laptop computers assigned to police personnel and E911 Communications Center Computer-Aided-Dispatch (CAD) systems are configured to access various law enforcement databases and networks, such as the national Criminal Justice Information Services (CJIS) and Florida's Criminal Justice Network (CJNet), etc.

2. Use of information in the system is strictly limited to law enforcement personnel and for law enforcement purposes only, and may not be disseminated to any person for any other purpose.

3. Use of law enforcement networks is restricted to only those personnel who have been trained and hold current 'digital' certificates and/or have appropriate access rights.

4. The sharing of 'digital' certificates is **STRICTLY PROHIBITED.**

XIII. MISCELLANEOUS

A. Data Security

1. Users must periodically save their computer files to prevent loss of data through accidental or unexpected computer mishaps, power interruptions or power outages.

2. Networked computer Users must save their files to their Home Directories, known as the H Drive, or City shared directories, and not to their local computer drives, such as Drive C or Drive D.

3. All data files stored in network home directories, department shared directories and City shared directories are backed up regularly. In order to comply with public records law, Users are responsible for copying and/or moving all files pertinent to City business to their appropriate home directories, and department or City shared directories.

4. Files stored on local computer hard drives or external media are NOT backed up by IT and the safety and integrity of such data is the sole responsibility of the individual User.

5. Users should be aware that once a hard drive crashes or any other medium containing electronic data (USB drives, floppy disks, etc.) is damaged, IT is UNABLE TO RECOVER any data and that the data is permanently lost.

B. System Maintenance

1. Users shall periodically perform routine clean-up procedures such as deleting unneeded files from their home directories and email accounts to ensure proper and efficient operations.

2. Users loading data (documents, folders, pictures, etc.) on the City's shared network directories are responsible for removing them when they are no longer needed or valid.

C. Downloading and Transmitting Information

1. Users shall be extremely cautious when downloading files. While the City computers have virus scanning software installed, it is not failsafe. It is strongly recommended that file downloads be kept to a minimum.

2. Users shall not download streaming audio or video files via Email unless they are used in conjunction with software applications and equipment approved by the Department Director and IT Management. If users require the use of streaming audio or video files for education, training or other business-related purposes, they shall contact their Department Director for approval and IT for access.

3. Downloading and installing screensavers, desktop and email wallpaper and mouse pointers are not authorized.

4. Questions regarding file downloads should be directed to the IT staff.

D. Access to Data Closets

1. IT staff must have access to all Data Closets located in City-occupied buildings on

campus and offsite to maintain network and telecommunications equipment and circuits, and resolve equipment-related problems as they occur.

2. The appropriate Department Director must provide the City Manager and IS Manager with a door access key and security alarm code if applicable to gain immediate or emergency access to Data Closet equipment and circuits.

SIGNING POLICY

All Users shall be required to read and sign the attached usage agreement in the presence of their Department Directors, Supervisors, or Human Resources staff acknowledging receipt and review of this policy.

A copy of the signed agreement shall be placed in the User's personnel file, if applicable, located in the Human Resources Department.

IT will periodically review this policy to ensure that it is current with technology in place.

APPENDIX A

CITY OF RIVIERA BEACH
COMPUTER, TECHNOLOGY, AND INTERNET USAGE POLICY
EMAIL POLICY

AGREEMENT FOR COMPUTER, TECHNOLOGY AND INTERNET USAGE

As an elected official, employee, or other authorized User of the City of Riviera Beach, I _____, recognize and understand that the City of Riviera Beach's Computer, Technology, Email and Internet systems are to be used for City business. The use of these systems for personal use is subject to the guidelines set forth in the City's Computer, Technology, and Internet Usage Policy.

I am aware that the City of Riviera Beach reserves the right to monitor any/all activities that take place on the City's Computer, Technology, and Internet systems with or without notice. I am also aware that by using the City of Riviera Beach's Computer, Technology, Email and Internet systems, I expressly consent to the monitoring of all electronic communications and Internet-related matters on these systems. Further, I am aware that the use of a City-provided password does not prevent the City of Riviera Beach from monitoring and accessing electronic communications and/or Internet-related matters.

I understand that violations of this policy may subject me to disciplinary action, up to and including termination of employment as outlined in the City's Policy for Discipline and Control and may result in a suspension or termination of privileges.

I acknowledge that I have received the above-stated City of Riviera Beach Computer, Technology, Email and Internet Usage Policy.

_____ _____

Elected Official, Employee, or other Authorizer User Signature Date

_____ _____

Witness Date

Departmental Sponsor: Finance & IT

Policy Review Date: November 2017

References: This Policy supersedes the email Section VIII of Policy #FN-14-003; Policy # IT-11-1; Resolution 3-11

Departments Affected: All

Approved By: Ruth C. Jones