

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<u>Subject:</u> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<u>Regulation No:</u> 1.17	<u>Effective Date:</u> June 1, 2012
	Supersedes: NEW	

**I. POLICY**

The Town of Vienna relies heavily upon internal and external electronic hardware and software information systems used to efficiently store, retrieve and process information. The security, reliability and integrity of the computer resources and information networks are of vital importance to the continued successful operation of the Town of Vienna, herein referred to as Town.

This policy addresses all employee use of the Town's computer hardware and software. The availability and use of personal computers within the work environment have provided many opportunities for enhancement of productivity and effectiveness. However, if not properly managed or used, these technologies can also have a damaging effect on the Town, its employees, and the public. Therefore, all Town employees shall abide by the requirements set forth herein when using Town's computers, the services of both internal and external databases, law enforcement networks, and the Town's electronic mail system.

**II. PURPOSE**

To establish rules and regulations designed to promote the effective and responsible use of the Town's computer resources.

**III. SCOPE**

This policy applies to all employees (hereinafter referred to as "users") who access or use the computer hardware, software and electronic mail resources provided by the Town of Vienna. Employees only shall use Town hardware; family members and others are not allowed to use employee workstations at work, home, or elsewhere via remote access. E-mail procedures are discussed separately in Policy 1.13. Internet procedures are discussed separately in Policy 1.14. Usage of these resources will be subject to other Town policies, including, but not limited to, Disciplinary Actions (2.15), Conduct of Employees (2.29), and Code of Ethics (2.30). Due to the special nature of their work, the Police Chief may place additional restrictions in relating to the operation of computers within the Police Department.

**IV. DEFINITIONS**

The following words and terms, whenever used or referred to in this manual, shall have the following respective meanings:

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<u>Subject:</u> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<u>Regulation No:</u> 1.17	<u>Effective Date:</u> June 1, 2012
	Supersedes: NEW	

**ACCESS:** To instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer networks.

**APPLICATION PASSWORD:** A password that a user may assign within an application and/or document in a Town computer that prohibits other users from opening the secured application or document.

**AUTHORIZED SOFTWARE:** Computer software developed, approved, purchased, or licensed by an agency of the Town of Vienna.

**BUSINESS CONTINUITY** (see also Disaster Recovery): The activity performed by the Town of Vienna to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. The foundation of business continuity are the standards, program development, and supporting policies; guidelines, and procedures needed to ensure the Town can to continue without stoppage, irrespective of the adverse circumstances or events.

**COMPUTER NETWORK:** Either a set of related devices connected to a computer by communications facilities, or a complex of two or more computers, including related devices, connected by communications facilities. This can be wireless devices and wired.

**COMPUTER SOFTWARE:** One or more computer programs, existing in any form, instructions, manuals, associated operating procedures, or other documentation. Software provides the instructions and controls through symbolic languages of the operation of all computers, including stand-alone and LAN (local area network) computers and related equipment as well as midrange computers.

**COMPUTER SYSTEM:** One or more connected or unconnected computers, peripheral devices, software, data, program, communications facilities, and computer networks. This can be wireless devices and wired.

**COMPUTER VIRUS:** A software executable code segment that is covertly incorporated into the executable program code files or data files of a computer or computer network and is activated when the host program executes. It can cause system degradation, including crashes, changes of data or complete erasure of hard drives.

**COPYRIGHT:** The rights granted to the owner of software by the Copyright Act, Title 17 of the U.S. Code. U.S. copyright law protects original tangible expressions, usually for 50 years beyond the creator's lifetime. This law was amended in 1980 to include computer programs.

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<u>Subject:</u> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<u>Regulation No:</u> 1.17	<u>Effective Date:</u> June 1, 2012
	Supersedes: NEW	

**DIRECTORY:** A directory is a named group of files that are separated by the naming convention from other groups of files.

**DISASTER RECOVERY (See also Business Continuity):** The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to the Town of Vienna after a natural or human-induced disaster.

**DISTRIBUTION DISK:** The original program CD's, and DVD's that are included with a software package at the time of purchase.

**FILE:** A file is an entity of data. Files can be program files, which contain instructions that allow the computer to perform various tasks under the control of the user, or data files, that contain information only. The file must have a unique name within its own directory.

**FILE SERVER:** A computer or device on a network that manages network resources and is dedicated to storing files. Any user on the network can store files on the server. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems, however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

**FOLDER:** Synonymous with directory, the term folder is more common in systems such as the Macintosh or Windows products which have a graphical user interface and provide a graphical file browser in which directories are traditionally depicted as folders.

**HARDWARE:** The parts of a computer system that you can touch. Examples of hardware are input devices like keyboards and mice, output devices like printers and monitors, storage devices like disk drives, and the computer itself.

**IMAGE:** In computer science an image is an exact replica of the contents of a storage device (a hard disk drive or CD-ROM for example) stored on a second storage device.

**LAN:** Local Area Network or a system served by one or more file servers. A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

**LICENSE AGREEMENT:** A contract between the software publisher and the intended user.

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<u>Subject:</u> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<u>Regulation No:</u> 1.17	<u>Effective Date:</u> June 1, 2012
	Supersedes: NEW	

**LOG-IN NAME:** The unique account name assigned to an access a computer system. Also called user ID or user name. A log-in name may be derived from the first several letters of the employee's last name and the first letter of his/her first name. (i.e., User: George Browne, Log-in Name: gbrowne.)

**LOG-IN PASSWORD:** A unique code or word linked to the log-in name that is used by an individual employee to gain access to a computer resource. Windows and e-mail passwords must be kept secret and not shared.

**MOBILE DATA:** A laptop computer used as a mobile workstation for field access to our network of information resources. The term is synonymous with the term workstation, as used throughout this policy.

**NETWORK OPERATION:** Logging onto or using a work station, application, or program linked to or installed on a file server.

**PORTABLE MEDIA STORAGE:** Extension of a hard drive which can store information on a variety of media including, but not limited to, thumb and/or flash drives, floppies, DVD's, CD's, memory sticks, and PDA's (Personal Digital Assistants) (i.e., Palm Pilot, IPOD, etc.).

**POWER-ON PASSWORD:** A password assigned to a computer that prevents other users from starting the system.

**SOFTWARE:** Software is the program that runs on a computer. Software is made up of instructions that tell the computer what to do. It is stored on portable media storage in bits and bytes.

**SYSTEM ADMINISTRATOR:** Person(s) responsible for the operation and maintenance of all software, workstations, file servers, and peripheral equipment. May also be referred to as the Information Technology Technician.

**USER:** Employee, any natural person, corporation, trust, incorporated or unincorporated association and any other legal entity or governmental entity, including any state or municipal entity or public official.

**VIRTUAL PRIVATE NETWORK (VPN):** A network that uses a public telecommunication infrastructure and their technology such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<b>Subject:</b> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<b>Regulation No:</b> 1.17	<b>Effective Date:</b> June 1, 2012
	Supersedes: NEW	

**WIRELESS NETWORKING:** Wireless networking refers to hardware and software combinations that enable two or more appliances to share data with each other without direct cable connections. Thus, in its widest sense, wireless networking includes cell and satellite phones, pagers, two-way radios, wireless LANs and modems, and Global Positioning Systems (GPS).

**WORK PRODUCT:** Any electronic document, spreadsheet, digital image, program, or other file that is created or produced on a Town resource.

**WORKSTATION:** All computer-related hardware including, but not limited to, processor, keyboard, monitor, printer, mouse, trackballs, scanners, digital imaging devices, modems, UPS devices, surge protectors, cables, connectors, adapters, telephones, and any other device attached to any component. Computers that are linked together to form a local area network (LAN), although they can also be used as stand-alone systems.

**V. SYSTEM ADMINISTRATION**

The Information Technology employees shall have administrative responsibility for all Town computer hardware, software and data resources.

**VI. USE OF COMPUTERS AND COMPUTERIZED INFORMATION**

The Town of Vienna prohibits the dissemination of Town owned or shared information, in any form, contained in or accessed through the Town's computers, to any other person, except one who is officially entitled to receive such information.

Accessing or attempting to access systems, files or documents belonging to the Town or a third party, when not related to the performance of your job assignment is prohibited. For example, attempting to access or view anything in the Town's information network for the purpose of satisfying curiosity is clearly inappropriate.

Employees learning of or suspecting any misuse of the Town's computer resources, including its hardware, software, related documentation, mobile data, or Requests for Electronic Data should alert the Information Technology Administrator or Town Manager.

**VII. REMOTE ACCESS POLICY**

The purpose is to define standards for connecting to the Town of Vienna's (hereinafter

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<u>Subject:</u> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<u>Regulation No:</u> 1.17	<u>Effective Date:</u> June 1, 2012
	Supersedes: NEW	

“Town”) communication networks from any host. These standards are designed to minimize the potential exposure to the Town from damages which may result from unauthorized use of the Town’s resources. Damages include the loss of sensitive or Town confidential data, intellectual property, damage to public image, damage to critical Town internal systems, etc.

This policy applies to all Town employees, contractors, vendors, and agents with a Town of Vienna-owned or personally-owned computer/device used to connect to the Town’s communication networks. This policy applies to remote access connections to do work on behalf of the Town, including reading or sending e-mail and viewing Internet, intranet, extranet web resources and all telecommuting situations.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

1. Use of remote access is restricted to authorized Town employees, contractors, vendors, and agents as designated by the Town Manager or his/her duly authorized designee and is for the sole purpose of conducting Town business.
2. The user shall review any related Town policy/policies for details of protecting information when accessing the Town’s communication networks via remote access methods, and acceptable use of the Town’s communication networks.
3. All hosts, including personal computers that are connected to the Town’s communication networks via remote access technologies must use the most up-to-date anti-virus software.
4. Personal equipment that is used to connect to the Town’s communication networks must meet the requirements of the Town for remote access.
5. Departments or individuals who wish to implement non-standard Remote Access solutions to the Town’s production networks must obtain prior approval from the Information Technology Administrator.

**VIII. IMPROPER USE OF COMPUTER SYSTEMS AND INFORMATION**

Improper use of computerized information includes the following non-exhaustive list of activities:

1. Obtaining information or using any Town resource in violation of law, regulation, policy,

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<u>Subject:</u> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<u>Regulation No:</u> 1.17	<u>Effective Date:</u> June 1, 2012
	Supersedes: NEW	

procedure, or other rule.

2. Release or use of records for personal or financial gain, or to benefit or cause injury to a third party.
3. Use of any Town resource for access to or distribution of indecent or obscene material or child pornography.
4. Harassing other users, or tampering with any computing systems, and/or damaging or altering the software components of same.
5. Use of Town resources for fundraising, commercial or political purposes, benevolent association activities, or any other activities not specifically related to a business necessity of the Town.
6. Any activity which adversely affects the availability, confidentiality, or integrity of any system resource and/or related data.
7. Engaging in acts that are deliberately wasteful of computing resources or which unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, broadcasting unsolicited mailings or other messages unrelated to the business necessity of the Town, creating unnecessary output or printing, or creating unnecessary network traffic.
8. Data accessed through third party resources, including, but not limited to, law enforcement networks, are regulated by a myriad of federal and state law and administrative regulations and shall be exclusively restricted to use by duly authorized employees and/or criminal justice agencies in the performance of their official duties. Employees shall adhere to all third party security agreements governing the authorized access and use of relevant databases.
9. All electronic traffic (email, Internet, instant message, WiFi, and so on) is subject to tracking and record archiving per user.
10. Do not view, sell or purchase merchandise for personal gain or operate a business utilizing Town electronic resources.

**IX. COMPUTER SOFTWARE**

It is the policy of the Town of Vienna to comply with all state and federal regulations

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<b>Subject: COMPUTER HARDWARE AND SOFTWARE USE</b>	<b>Regulation No:</b> 1.17	<b>Effective Date:</b> June 1, 2012
	Supersedes: NEW	

governing the use of computer software. Illegal or unauthorized use of software may have severe consequences, including legal action for an injunction barring further use of the software and actions for monetary damages and penalties.

In most cases, the Town does not own all rights to software developed by a third party. Instead, the Town's rights are governed exclusively by a license agreement. Unless expressly authorized by the license agreement, the Town does not have the right to reproduce either the software or its related documentation. It is the policy of the Town to respect all computer software copyrights and to adhere to the terms of all software licenses to which all departments within the Town and its employees, are a party.

The Town prohibits the illegal duplication or use of computer software, whether developed by its own employees or by third parties.

Each employee using original issue, commercial copyrighted software shall do so only in accordance with any applicable license agreement and departmental policy. Town proprietary software is to be used only to conduct the Town's business and is not to be copied for personal use or transferred to third parties for use without administrative authorization and without execution of appropriate licensing documentation. Upon termination of employment, the employees shall return to the Information Technology Administrator or departmental supervisor all department and third party software in their possession.

Employees learning of such misuse of software or related documentation or have questions pertaining to said same should contact the Information Technology Administrator or the Information Technology Administrator's office.

**X. PURCHASING/MODIFYING/INSTALLING COMPUTER SOFTWARE OR HARDWARE**

Since software programs installed on the local hard drive or other devices may interact negatively with existing programs (running either from a workstation or a file server), only software authorized by the Information Technology Administrator, IT Technician or the Town Manager will be installed, loaded, or otherwise used on a Town workstation.

**XI. NO PRIVACY EXPECTATION FOR THE TOWN'S COMPUTER FILES**

Employees have no expectation of privacy beyond those accorded non-employees in the files stored on the Town computers, networks, tapes, or removable media. These files may be accessed



**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<u>Subject:</u> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<u>Regulation No:</u> 1.17	<u>Effective Date:</u> June 1, 2012
	Supersedes: NEW	

by the Town's technical or supervisory personnel without notice.

The assignment or use of a system password implies no ownership rights or any expectation of privacy on any Town computer resource.

Supervisors needing to access any password protected or encrypted files of an absent employee in order to facilitate the business needs of the Town shall contact the Information Technology Administrator. An employee shall provide all keys or passwords to files that have been encrypted or password protected upon request of either the Information Technology Administrator or the Departmental Supervisor.

**XII. USE AND CARE OF EQUIPMENT**

Employees are reminded that the Town's workstations are of vital importance to the productivity of the Town. These costly and environmentally sensitive electrical devices require proper use and care. Do not damage hardware, electronic systems, or networks.

**XIII. OPERATIONAL GUIDELINES**

**A. Generally:**

- Employees shall not delete, erase, alter or format drives, directories, disks, files or folders created by the Information Technology Administrator or user without the authority to do so from the Information Technology Administrator, Department Head or Supervisor.
- Employees shall not copy or otherwise create an image of any program without authorization of the Information Technology Administrator.
- Employees shall not copy or otherwise create an image of any file not specific to the performance of their job requirements without authorization of the Information Technology Department.
- Only software authorized by the Information Technology Administrator, IT Technician or the Town Manager will be installed, loaded, or otherwise used on a Town workstation.
- Software authorized for use must be scanned for virus contamination and installed by the Information Technology Administrator. Employees will not configure, modify, partition, or alter any predefined hardware or software configuration setting, including, but not limited to, the CMOS/MOS setting, registry or hard disk, located in any Town computer resource. Employees experiencing difficulty in operating a workstation should not turn off or unplug the computer without first contacting the Information Technology Administrator.

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<u>Subject:</u> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<u>Regulation No:</u> 1.17	<u>Effective Date:</u> June 1, 2012
	Supersedes: NEW	

- No computer shall be equipped with or attached to an external communication device designed for remote operation or connection (i.e., a modem) without prior written authorization from the Information Technology Administrator.
- In order to prevent unauthorized access to the Town’s computer system from an outside source, any desktop computers equipped with network access and an external communication device (i.e., a modem) shall not be left powered on during non-working hours, unless authorized by the Information Technology Administrator.
- The unauthorized operation of any system resource while utilizing a password or access privilege other than an employee’s own is prohibited.
- In the interest of security, employees shall not leave desktop workstations unattended without logging/signing off or the setting of a screensaver.
- Employees discovering any security violations or system vulnerabilities shall immediately notify the Information Technology Administrator so that corrective action can be taken.
- It is the responsibility of employees assigned to vehicles equipped with computers to safeguard such devices. Vehicles so equipped will be locked at all times when the vehicle is unoccupied.
- The Information Technology Administrator should be immediately notified if a mobile workstation, or any hardware or software, has been stolen, or unauthorized access was attempted or gained, in order to implement procedures to safeguard the integrity of our networked resources or other digital resources.

**B. Portable Media Storage (“PM Storage”)**

Because any user can come into the office, plug in a USB stick the size of the average keychain and take in/out 1GB (or more) of data it poses a tremendous threat. Users can take confidential data or they can introduce viruses, Trojans, illegal software and more – actions that can affect the network and the Town severely.

Due to the high security risk, only authorized employees may utilize PM Storage for Town business. Personal use of PMS on Town-owned computers is strictly prohibited. For business use, a request must be made to the department director for the use of PM Storage and include a valid business reason for such use. The department director will inform the Information Technology Manager of any authorized users within their department.

The Town of Vienna has invested in network anti-virus software, firewalls, email and web content security. Because of this PMS must be scanned prior to use, especially if the user has used the device on a non Town-owned computer prior to using it at the Town.

**TOWN OF VIENNA, VIRGINIA  
ADMINISTRATIVE REGULATIONS**

<u>Subject:</u> <b>COMPUTER HARDWARE AND SOFTWARE USE</b>	<u>Regulation No:</u> 1.17	<u>Effective Date:</u> June 1, 2012
	Supersedes: NEW	

Only Town issued PM storage units are to be used.

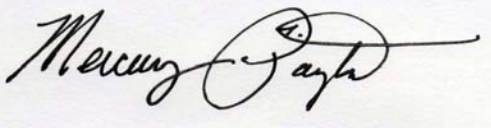
**C. Disposal or Re-use of Computer Related Media Containing Information Overview**

When use or retention of any media containing any information (including protected or confidential information) is completed, the information must be destroyed, rendered unrecoverable, or given to I.T. for proper handling. In general, other electronic media (hard drives, DVD, CD, floppy disk, zip drive, thumb drive, etc.,) must be physically destroyed to be rendered unreadable.

If electronic media contains electronic protected information or other confidential information, the hard drives must be zeroed or degaussed before the computing device is recycled to another user and/or before it is taken out of service at the Town.

**XIV. PASSWORDS**

An employee's password is the first line of defense against unauthorized use of an employee's assigned computer resources. If someone guesses or otherwise acquires an employee's password, that individual can impersonate that employee. This embarrassing situation will compromise the integrity of the Town's computer system resources. Employees shall keep their passwords secure at all times. Passwords should never be taped to the bottom of keyboards, monitors, workstations or work places.

<i>Signature of Town Manager:</i>	<i>Date:</i>
	June 1, 2012