VILLAGE OF FORSYTH, ILLINOIS

VILLAGE OF FORSYTH, ILLNOIS
TECHNOLOGY POLICY

Section 1: PURPOSE

This policy covers the use of electronic technology resources belonging to, or used by the Village of Forsyth (the "Village"). It includes, but is not limited to, all computer systems, software, copiers, typewriters, scanners, network resources, fax machines, cell phones and internet resources. All technology resources owned by the Village are Village property and are in place to enable the Village to provide its services in a timely and efficient manner. This is the primary function of these resources and any activity or action that interferes with this purpose is prohibited. Because technology systems are constantly evolving, the Village requires its employees to use a common sense approach to the rules set forth below, complying not only with the letter, but also the spirit, of this policy.

Section 2: DEFINITIONS

Electronic technology resources: include, but are not limited to, host computers, file servers, routers, firewalls, switches, hubs, workstations, stand-alone computers, laptops, printers, scanners, software, internal or external data communication networks, cell phones, electronic notebooks, flash drives and fax machines.

Users: as used in this policy, refers to all employees, elected and appointed officials, independent contractors and other persons or entities accessing or using any of the Village's electronic technology resources.

Email: is the ability to compose and distribute messages, documents, files, software, or images by electronic means over a phone line or network connection. This includes internal and external email and instant or text messaging systems.

Software: is the computer programs that reside on any type of computer or electronic device including equipment control systems to perform a desired function. It encompasses programs provided by the manufacturer, a vendor or developed by in-house staff.

Network resources: includes the hardware and software necessary to connect computers and resources into a communication system.

Internet: is the worldwide network of computer servers that allow access to the public through the use of special languages.

Section 3: SCOPE

This policy shall apply to all users of the Village's electronic technology resources.

Section 4: OWNERSHIP AND PRIVACY EXPECTATIONS

All technology resources and all information transmitted by, received from and stored on the Village's computer system is the property of the Village and as such, are subject to inspection by Village officials. Users of the Village's electronic technology resources do not have an expectation or right of privacy. The network administrator has the right to audit and monitor the information on all systems, electronic mail and information stored on computer systems or media, without advanced notice. This might include, but is not limited to, investigation of theft, unauthorized disclosure of confidential business or proprietary information, personal abuse of the system or monitoring workflow and productivity.

- The use of the Internet is restricted to official Village business. Personal use of or time spent for personal gain is strictly prohibited. Authorization for Internet access must be obtained through your immediate supervisor. Once authorization is approved you are responsible for the security of your account password and you will be held responsible for all use or misuse of your account. You must maintain secure passwords and never use an account assigned to another user.

- Hacking is the unauthorized use or entry into any other computer. Never make an unauthorized attempt to enter any computer. Such an action is a violation of the federal Electronic Communications Privacy Act. 18 U.S.C. §§ 2510 - 2522.

- Sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited.

- The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.

- Never copy or transfer electronic files without permission.

- Downloading a file from the Internet can bring viruses with it. Scan all downloaded files with anti-virus protection software.

- Never send, post, or provide access to any confidential Village materials or information.

- Almost all data and software is subject to federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to you. Software which requires purchase or reimbursement for its use, such as

shareware, requires strict adherence to the terms and conditions specified by the owner unless written permission for unrestricted use has been obtained. When in doubt consult your network administrator.

- You are obligated to cooperate with any investigation regarding the use of your computer equipment which the network administrator has authorized.

- Chain letters are illegal and may not be transmitted through email.

- Email requires extensive network capacity. Sending unnecessary email, or not exercising constraint when sending very large files, or sending to a large number of recipients consumes network resources that are needed for critical Village business. When the Village grants an individual employee access to the network, it is the responsibility of the employee to be cognizant and respectful of network resources.

- Email on the network is not secure. Never include in an email message anything that you want to keep private and confidential because email is sent unencrypted and is easily read. Do not use email for confidential communications without approval of the network administrator.

- The network administrator has the right to access all email files created, received or stored on the Village's network system and such files can be accessed without prior notification.

- Email created, sent, or received through the use of any Village owned resource is the property of the Village, not its employees.

- Users can have no expectation or rights of privacy in anything they create, send, store, or receive on any Village-owned electronic technology resource. Be aware that the recipient of a message may forward it to any number of other parties. Email may become evidence in a lawsuit. A good rule is to compose email with the expectation that it will become public. The Illinois Attorney General regards email as a public document. In other words, don't create or send an email that you might not want someone else to see.

Section 5: PERSONAL USE

Personal use of the Village's electronic technology resources is allowed with the following restrictions:

- Employees should be aware that personal use of a Village technology resource is still subject to all rules in this policy including inspection and monitoring.

- Use must be conducted on an employee's own time during lunch and breaks.

- Use must not interfere with other employees performing their jobs or undermine the use

of the Village's resources for official business.

- Use of the Village's electronic technology resources for operating a personal business is prohibited.
- Personal use of the Village's electronic technology resources neither expresses nor implies sponsorship or endorsement of such use by the Village.

- Sending or forwarding jokes, chain letters or large images is prohibited.

- All personal use of Village electronic technologies must not be used in any manner that may be construed as harassment or discrimination.

Section 6: PASSWORD PROTECTION

All employees and personnel that have access to Village owned computer systems must adhere to the password policies defined below in order to protect the security of the entire network, protect data integrity, and protect the overall computer network system.

- Never write passwords down

- Never send a password through email

- Never include a password in a non-encrypted stored document

- Never reveal your password over the telephone

- Never use the "*Remember Password*" feature of application programs such as Internet Explorer, your email program, or any other program you may be using

- Never use your Village password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://

- Report any suspicion of your password being broken to the network administrator

- Don't use common acronyms, part of your login, your name, names of people or familiar places, pets, as part of your password

- Passwords should be at least eight (8) characters in length and should be case sensitive

- Passwords should contain at least one (1) special character (#, $, %, *)

- Do not share your password with anyone

- Passwords should be changed every three (3) months

- Passwords will be stored using reversible encryption

Section 7: REMOTE ACCESS

A remote access policy is designed to prevent damage to the Village of Forsyth network and to prevent compromise or loss of data. Any remote access using either dial-in, VPN, or any other remote access to the Village network must be reviewed and approved by the Village Administrator. All employees by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access.

Section 8: SYSTEM BACKUPS

Full backups are performed nightly, Monday through Friday. There shall be separate external hard drives used for performing these backups. External backup drives are alternately used and kept off-site when not in use.

Section 9: LAPTOP SECURITY

Users will accept the responsibility for taking reasonable safety precautions with the mobile computer and agree to adhere to this policy. The user will not be allowed to have administrative rights unless granted a special exception by the network administrator. Users agree not to use the mobile computer for personal business and agree to abide by the organizational computer usage policy.

Devices connected to the Village's network must be determined to be a benefit to the Village of Forsyth rather than convenience by the designated IT manager. All mobile devices owned by the Village or allowed on Forsyth's network must be identified by their MAC address to the network administrator before connection is allowed.

Devices not owned by the Village of Forsyth are subject to a software audit to be sure no software that could threaten the network security is in operation. All competing devices are subject to a software audit at any time.

Do not download, install or use unauthorised software programs. Unauthorized software could introduce serious security vulnerabilities into the Village of Forsyth's network as well as affecting the working of your laptop. Software packages that permit the computer to be 'remote controlled' (*e.g.* PCanywhere) and 'hacking tools' (*e.g.* network sniffers and password crackers) are explicitly forbidden on any Village of Forsyth's equipment unless they have been explicitly pre-authorised by the Network Administrator for legitimate business purposes.

Be careful about software licences. Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being

prosecuted for infringing software copyright: do not risk bringing yourself and the Village of Forsyth into disrepute by breaking the law.

Access rights to the Village's network cannot be transferred to another person even if that person is using an allowed computing device. The device must meet the computer connection standards determined by the Network Administrator.

Section 10: DISASTER RECOVERY PLAN

Develop a disaster plan to be reviewed annually to ensure its relevance. For this purpose, a planning team that includes the Village Administrator, all department heads, attorney, and the network administrator will work together to develop the plan and review it each year. Their roles and responsibilities will include:

- Discuss risk assessment to determine information system vulnerabilities.
- Perform a business impact analysis to document and understand the interdependence among department processes and determine how each one would be affected in the event of an information technology outage.
- Take an inventory of information technology assets infrastructure.
- Identify critical applications, systems and/or data.
- Prioritize key department systems
- Ensure critical applications, systems and/or data are distributed to facilities that are reasonably able to access in the event of an outage.
- Assign one member of the team to make critical decisions as necessary.
- Develop testing standards of the plan. Provide documentation of these standards.
- Provide security awareness and disaster recovery education to all members of the team.
- Perform continuous computer vulnerability assessments and audits.

Section 11: POLICY VIOLATIONS

Examples of violations of this policy include, but are not limited to, the following:

- Soliciting or advertising for personal or commercial gain;
- Soliciting or advertising for outside organizations, such as religious, charitable or political causes; (exemptions may be made for organizations such as United Way, Muscular Dystrophy Association, etc. and other agencies with prior approval from the

network administrator);

- Creating, sending, viewing, faxing, and storing messages and/or websites that may reasonably be regarded as offensive, obscene, disruptive, illegal, fraudulent, profane, embarrassing or libelous. These include information that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability or religious or political beliefs. Users encountering or receiving such material should immediately report the incident to their Supervisor;

- Sending or forwarding email or fax material either internally or externally, without identifying yourself clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden;

- Attempting to access another employee's email without permission;

- Using another employee's access code to view, alter, or distribute information without the express authorization of that employee;

- Using Village electronic technology resources to access sensitive or confidential information, as well as using said sensitive or confidential information in a manner not originally intended;

- Installing local employee-owned or non-Village purchased software on Village electronic technology resources, whether intended for legitimate business matters, personal purposes, or amusement, This includes, but is not limited to, shareware, freeware, personal software, stealthware, and internet distributed programs;

- Altering, adding or removing any Village technology resources without clearance and approval from the network administrator;

- Downloading files from any source and not scanning for viruses. This includes files obtained as email attachments or by any other file transfer mechanism. It is the responsibility of users to take prudent steps to prevent the introduction or propagation of viruses;

- Using electronic resources in any illegal, malicious or inappropriate manner;

- Transmitting confidential personal information using email systems or the fax machine;

- Using personal software without the approval of the network administrator.

If the Village determines that an employee has used electronic technology resources in a manner that violates this policy or other state or federal law, the violation may result in disciplinary action up to and including termination, as outlined in the Village's Personnel Policy.

Section 12: APPROPRIATE USE

At all times when a user is using the Village's electronic technology resources, he or she is representing the Village. Users should exercise the same good judgment in all resource use that they would use in written correspondence Users are expected to use Village-provided electronic technology resources responsibly and professionally.

Failure to follow guidelines as set forth in this policy may result in disciplinary action up to and including termination.

The Village is not responsible for the actions of individual users.

This policy may be amended or revised periodically as the need arises.

Policy approved by the Mayor and Board of Trustees on May 21, 2012.

Mayor

ATTEST:

Village Clerk