Title:	Use of Village Facilities & Equipment
Chapter:	Information Systems (IS) Policies & Procedures
Policy Number:	7.3
Creation Date:	March 1, 2001
Issued By:	Manager of Information Systems & Assistant Village Administrator
Approved By:	Village Administrator
Last Revised:	December 16, 2013

I. GENERAL

A. PURPOSE

1. To establish guidelines for electronic devices and network usage for the Village. To provide operational guidelines for all Information System ("IS") resource users who are engaged in electronic data processing related activities. These Information Systems Policies (the "Policies") shall apply to all Users of the Village's IS resources (collectively and hereinafter referred to as the "System").

2. The Policies apply to the use of all desktops, workstations, laptops, PDAs and cellular devices, servers, and internal or external communication networks, including but not limited to electronic devices, tablets, terminals, and all forms of peripherals (e.g., printers, modems, scanners, and drives) that create Data, and are accessed directly or indirectly by means of the System.

3. Prior to being granted access to the Data and the System, including the Electronic Mail System and the Internet, a User must have on file a signed statement that he or she has read and understands the Village's Information Systems Policies. Such signed statement shall be placed in the User's official Personnel file.

II. DEFINITIONS

A. DATA: The term Data means any and all information created, received, distributed, transferred, and stored on the System, including, but not limited to, system and application software.

B. ELECTRONIC COMMUNICATION: The term Electronic Communication refers to both Electronic Mail (E-Mail) and Voicemail, both of which are privileged communications systems that electronically creates stores, and forwards communications and Data, from one User to one or more Users.

C. MIS: The term MIS means the Village's Manager of Information Systems

D. SYSTEM: The term System means any and all of the phones, desktops, workstations, laptops, PDAs and cellular devices, servers, and internal or external communication networks, including but not limited to electronic devices, tablets, terminals, and all forms

of peripherals (e.g., printers, modems, scanners, and drives) that create Data, and are accessed directly or indirectly by means of the Village System.

E. USER: The term User means anybody authorized by the Village to access or use the System, including but not limited to elected officials, employees (as defined by the Employee Personnel Manual), committee and commission members, consultants, contractors, vendors, and volunteers.

III. GUIDELINES

A. At the Village Administrator's sole discretion, the Policies may be revised as presented or new policies may be created. All new policies are to be submitted to the Village President and Board of Trustees for their review.

B. The Village Administrator is responsible for administering these Policies and for the planning, implementation, management and maintenance of the System and related activities.

C. New or revised policies will be formulated and proposed by the MIS to the Village Administrator. All proposed new or revised policies shall be submitted to the Department Directors by the Village Administrator or an authorized designee for review and comment

D. New or revised policies may be derived from many varied sources, including employee suggestions. Suggestions for any new or revised policies shall be forwarded to the MIS for consideration.

E. Prior to being granted access to any Village Information System, a User must have on file a signed statement that they have read and understand this Policy. Said signed statement shall be placed in the User's Personnel File.

F. Users should not have an expectation of privacy for any Data created, sent, received, or viewed on the System.

G. The Village has the right, but not the duty, to monitor any and all aspects of the System to ensure compliance with these Policies and all applicable state and federal laws. Such monitoring by the Village may occur at any time with no requirement to provide advance notice to the User. Access to the System is given to Users to assist them in the performance of their work related duties. The System and the Data belong to the Village.

H. Any conflicts between these policies and other sections of the Village's Employee Personnel Manual shall be resolved by the Village Administrator.

I. These Policies shall apply to all Users of the System wherever located. Any violation of these Policies shall result in disciplinary action up to and including dismissal and/or legal action. Access to the System provided by the Village is a privilege that should not be abused by any User.

J. The Village reserves the right to terminate a User's access to the any or all System resources at its sole discretion.

K. Without proper authorization, the MIS or other IS personnel are not authorized to open files with a user's system folder. Said authorization shall come from the individual, the individual's Department Director, and/or the Village Administrator. Authorization to open the Village Administrator's files shall be granted by the individual or the Village President. Authorization to open an elected official's files shall be granted by that particular elected official, or by a vote of a majority of the corporate authorities holding office.

L. Any requests from the Freedom of Information Officer to open files of other Users on the system will be submitted to and can only be approved by the Village Administrator or by the Village President if the office of Village Administrator is vacant.

IV. SECURITY

A. PURPOSE

To ensure that the System is secure and protected from damage due to tampering, vandalism or other attempts to destroy or access Data and/or equipment, without approval.

B. GUIDELINES

1. Users shall use and/or disclose Data only as is required for the proper performance of their work related duties unless otherwise provided for in these Policies.

2. The Village has licensed and/or purchased all software, applications, operating systems, and equipment for the explicit and sole use to conduct Village business.

3. Users shall comply with all applicable license agreements, with all state and/or federal laws governing the System, and with all applicable copyright, trade secret or other intellectual property right laws.

4. Access to, changes to and separation from the System shall be requested as follows:

    a. The Department Director shall notify the MIS to add a new user account, or to change an existing user account along with a description of the System and Data access that the new or existing user will require.

    b. The MIS shall contact the new User's Department Director to inform the Director of the activation of the user account.

    c. Upon a User's separation from the Village, the Department Director shall immediately inform the MIS of the separation. The MIS shall disable the user account in question and place the former User's data in control of the former User's Department Director.

5. Users will be provided login credentials, which allow access to permitted content of the System. The User will then provide a personalized, confidential network password. The confidentiality of the network password is the sole responsibility of each User. Network passwords should not be printed, stored on-line, or given to others. Users of the System shall be required to change their network password at

regular intervals as directed. The network password will be a minimum of six (6) characters in length and include lower-case letters, upper-case letters, numbers, and/or characters.

6. No User shall be required to divulge his or her personalized, confidential network password. No Department shall maintain a list of passwords. Any person with knowledge of any network password not their own shall immediately report this to their supervisor or the MIS.

7. Users may password protect any document as authorized or directed by their respective Department Director. In all instances where a User has password protected a document, that User will be required to provide the document password to the respective Department Director. Said Department Director shall maintain a list of these document passwords using proper security and control.

8. To maintain the security of the System, all Users are required to lock or logout of the System when they are not in physical control of the computer from which they have gained access. Failure to do so may jeopardize the integrity and/or security of the Data, including but not limited to unauthorized changes to Data, unauthorized access to sensitive/confidential information, and inappropriate E-mail messaging. Users are responsible for all transactions made using their login credentials.

9. Unless expressly authorized and approved by the appropriate Department Director or otherwise provided for in these Policies, no User shall access information during working hours that is not directly related to his or her assigned daily work related duties

10. In order to protect the System from computer virus and malicious software that may be introduced, anti-virus software is required on any desktop, workstation, laptop, or other device capable of the reading and writing of Data to the System. The Village will determine, purchase, install, and maintain the anti-virus software for Village owned devices. The software shall not be disabled by any User.

11. The Village reserves the right to install and maintain any hardware, software or physical controls to ensure the security of the System and Data. The Village reserves the right, without prior notice to or approval of any User, to access and disclose the Data and files contained on the System and on any computer, storage medium, or other electronic device.

12. All servers shall have a security system installed and enabled.

13. It is the responsibility of the MIS to ensure that the security system is operable and maintained on each device attached to the network.

14. Limited personal use of the System by Users is permitted during breaks and non-working hours as long as the use does not (1) interfere with the User's work performance; (2) interfere with any other individual's work performance; (3) have undue impact or cost on the operation of the System; or (4) violates any other provision of these Policies or any other policy of the Village. At all times, Users have the responsibility to use the System in a professional, ethical and lawful manner. Personal use of the System is a privilege and violations shall result in disciplinary

action up to and including dismissal. Other criminal or personal liability actions by the Village will be taken as appropriate.

15. No User shall install any software program and/or application into the System without prior approval from both the User's Department Director and the MIS, with the exception of allowing operating system, productivity, and security updates, patches, and software configured to automatically download and install. Configurations are maintained by the MIS. The User shall be responsible for contacting the Information Systems Division if there is a question in regards to installations.

16. No User shall place any Data or software that does not originate from the System, into the System without allowing the anti-virus software to scan the Data or software for viruses. Scanning for viruses shall be performed by the anti-virus software installed on the System.

17. No User shall attempt any unauthorized access to Data or programs via unauthorized login or password use.

18. Users who suspect unauthorized use or access of the System, Data or programs shall report such use or access to their supervisor, Department Director or the MIS immediately. Upon notification from the supervisor or Department Director, the MIS shall secure the System.

19. The Village reserves the right to disable any program if the security of the Data or System is at risk as determined by the MIS. The MIS shall notify the Village Administrator and Department Directors.

20. Users may not disrupt the operation of the System through abuse of or by vandalizing, damaging or disabling any component of the System.

21. A User shall not alter any Data belonging to another User without first obtaining permission from the individual creating or maintaining the Data. A User shall not copy Data belonging to another User without first obtaining permission from the owner or the owner's Department Director. The ability to read, alter, or copy Data belonging to another User does not imply permission to read, alter, or copy Data.

22. No User shall attempt to copy and/or transfer any Data to removable media without the expressed consent of the respective Department Director. Prior to utilizing any removable media, the User shall confirm to the MIS that the media is free of viruses and/or malware. Removable media shall mean any data storage device that can be detached or removed from the System, including but not limited to Smartphones, tablets, USB flash drives, USB/FireWire Hard Disks, Writable CDs or DVDs, etc.

V. ELECTRONIC COMMUNICATION

A. PURPOSE

To provide guidelines for the secure, effective and efficient use of the Village's Electronic Mail (E-Mail) and Voicemail. All Users are expected to communicate via E-Mail or

Voicemail in a professional manner that will reflect positively on themselves and on the Village.

B. GUIDELINES

1. All E-Mail and Voicemail messages are the property of the Village.

2. All E-Mail Users will be provided with a Village e-mail address in the following general format:

   "last name(first initial)@vil.bloomingdale.il.us"

3. No other E-Mail address will be permitted to be installed on the Village system, unless created by the MIS.

4. In using E-Mail and Voicemail, Users explicitly acknowledge that any message can be retrieved from the System, regardless of the User's action taken on their own messages. The Village is required by applicable State and Federal Laws to archive all E-Mail messages originating from the System and those received by the Village.

5. Users shall not forward any form of communication deemed confidential and/or privileged to any other person or entity that is not authorized to receive it, whether the person or entity is located inside or outside the E-Mail or Voicemail System, without the express permission of their immediate supervisor, Department Director or Village Administrator.

6. Users shall use care in preparing and disseminating any electronic communications. Anything created, distributed, or stored on the System may be reviewed by others. Any E-Mail will be attributed to the User's log-in credentials. All E-mail received by the System servers shall be filtered for spam, inappropriate material, viruses and malicious software.

7. Incidental and occasional personal E-Mail messages are permitted during breaks and non-working hours as long as such usage is in accordance with these Policies. These messages shall abide by the same guidelines for E-Mail, and Users are advised that the Village specifically reserves the right to retrieve and review any personal E-Mail messages on the System.

8. No User shall attempt any unauthorized access to E-Mail or Voicemail via unauthorized login or password use, or by misrepresenting their identity.

9. No User shall use E-Mail for the transmission or storage of games, personal advertisements, opinions, requests or business solicitations or any other unauthorized use. The Village reserves all rights to any material stored on the System and will remove any material which the Village, in its sole discretion, believes may be objectionable. If such use is detected, the User may lose E-Mail privileges and shall be subject to disciplinary action, up to and including dismissal and/or legal action. Examples of unauthorized usage of the E-Mail include, but are not limited to:

   a) Transmitting or storing fraudulent, embarrassing, indecent, profane, obscene, unlawful, abusive, threatening, or harassing messages or files, including those containing racial epithets, ethnic slurs, or any other language involving harassment

of others based upon race, sex, national origin, religion, disability, age, marital status, sexual preference, or based on other protected status under federal or state laws.

b) Transmitting or possessing sexually explicit material.

c) Transmitting or storing electronic files in violation of licensing agreements, state and/or federal laws governing E-Mail, or any applicable copyright, trade secret or other intellectual property right laws.

d) Transmitting chain letters.

e) Engaging in solicitation for non-work-related commercial, religious, political, fund raising or other causes, or any illegal activities.

f) Engaging in any improper activity that could adversely affect or discredit the Village.

10. No User, with authorized access to E-Mail and Voicemail, shall allow an unauthorized individual, group or entity to use the System E-Mail or Voicemail.

11. Without proper authorization, the MIS or other IS personnel are not authorized to open E-mails and Voicemails of other Users on the system, (excluding E-mails that have been quarantined by the system or are undeliverable as addressed). Said authorization shall come from the individual, the individual's Department Director, and/or the Village Administrator. Authorization to open the Village Administrator's files shall be granted by the individual or the Village President. Authorization to open an elected official's files shall be granted by that particular elected official, or by a vote of a majority of the corporate authorities holding office.

VI. INTERNET USAGE

A. PURPOSE

1. To define the use of and access to the Internet through the System.

2. All Users are expected to use the Internet in a professional manner that will reflect positively on them and on the Village.

B. GUIDELINES

1. No User shall attempt any unauthorized access to the Internet via unauthorized login or password use or misrepresent their identity.

2. No files shall be downloaded from the Internet to the System without the approval of the User's immediate supervisor, unless the file/s is in direct relation to the User's work related duties. The MIS shall have the ability to monitor any device attached to the System for files that have been downloaded from the Internet. These files shall be subject to deletion from the System without notice.

3. Internet usage may be limited to certain time periods, as well as length of time connected per day. The User's respective Department Director shall determine these limits.

4. The Village's use of the Internet is intended to be primarily for business purposes, although limited use during breaks and non-working hours may be permitted by the User's Department Director, the Village Administrator, or an authorized designee, in accordance with the guidelines described herein and in these Policies.

5. The Village's Internet connection shall not be used for personal entertainment, employment outside of the Village, or for any type of personal profit, including, but not limited to, accessing gaming sites, developing web sites, or for posting opinions or statements to publicly accessible resources, such as news groups, blogs, and social networking sites.

6. No User shall install, or cause to have installed, software that hides the User's identify from the MIS (i.e. proxy software).

7. The Village has implemented website filtering on its System to protect itself from malicious and rogue websites. The filtering software blocks unwanted, damaging, and inappropriate websites from being accessed. In its sole discretion, the Village may cause Users who attempt to access sites and/or addresses on the Internet that contain information or materials that are deemed to be inappropriate, to lose Internet access privileges and shall be subject to disciplinary action up to and including termination. Other criminal or personal liability actions by the Village will be taken as appropriate.

8. Examples of unauthorized Internet use include, but are not limited to:

    a) Transmitting or storing fraudulent, embarrassing, indecent, profane, obscene, unlawful, abusive, threatening, or harassing messages or files, including those containing racial epithets, ethnic slurs, or any other language involving harassment of others based upon race, sex, national origin, religion, disability, age, marital status, or sexual preference.

    b) Transmitting, possessing, or accessing sexually explicit material and/or sites.

    c) Transmitting or storing electronic files in violation of licensing agreements, state and/or federal laws governing the Internet, or any applicable copyright, trade secret or other intellectual property right laws.

    d) Transmitting chain letters.

    e) Engaging in solicitation for non-work-related commercial, religious, political, fund raising or other causes, or any illegal activities.

    f) Attempting to access any computer system, files, or messages without proper authorization.

    g) Engaging in any improper activity that could adversely affect or discredit the Village.

VII. USE OF NON-VILLAGE OWNED COMPUTER EQUIPMENT

A. PURPOSE

To establish guidelines for non-Village owned electronic data processing equipment and its connection to and use with the System.

B. GUIDELINES

1. Vendors, contractors, and consultants (collectively “Guest Users”) intending to connect to the System from non-Village owned computer equipment or systems shall be required to take certain precautions to ensure the integrity and security of the System. Guest Users shall notify the Supervisor in charge of their intent to connect to the System prior to connecting. The Supervisor shall notify the MIS to request approval.

2. Prior to permitting access to the System using non-Village owned equipment, the MIS is responsible for verifying that these Policies have been complied with.

3. As determined by the MIS, the Village reserves the right, at its sole discretion, to approve or deny Guest Users access to the System.

4. All software, hardware (i.e. -modem, network card, patch cords, printers, scanners, zip drives, any other peripherals) or other materials or services necessary to enable Guest Users to access the System shall be the full responsibility of the respective owners of said equipment.

5. The MIS shall review and approve the configuration of any Guest Users prior to accessing the System. Said review and approval is required upon any and all changes to the configuration of non-Village owned computer equipment.

6. The Village reserves the right, with the recommendation of the MIS and approval by the Village Administrator, to access and disclose any and all Data and files contained on Guest User’s equipment used to gain access to the System. Such access may occur for any reason, including but not limited to the Village's need to investigate a possible violation of policy or breach of the System's security. Any Data or files obtained under these guidelines may be disclosed without the consent of the Guest Users.

7. Guest User’s equipment that will be connecting to the System is required to have anti-virus and anti-malware software installed and configured appropriately, prior to accessing the System. Said software shall not be disabled during the time the equipment is connected to the System. The Guest User shall request the MIS to verify and confirm that the anti-virus and anti-malware software complies with Village standards.

8. The Village requires specific anti-virus and anti-malware software programs to be installed, as determined deemed appropriate by the MIS.

9. Guest Users are solely responsible for any and all repairs to their computer equipment in the event said equipment experiences operational, hardware or software failure for any reason. In the event that Guest User's equipment damages the System for any reason, the Guest User is solely responsible for the costs associated with any and all repairs and/or replacements to the System.

10. These guidelines apply to all Guest Users with a personally owned or company owned computer equipment used to connect to the System in order to access the Village's network resources, including but not limited to: data, internet, peripherals, etc.

VIII. REMOTE ACCESS

A. PURPOSE

To establish guidelines for connecting to the System from any User not directly connected to the System.

B. GUIDELINES

1. No User shall have or attempt access to the Village's network without express written consent of their Department Director.

2. Users should not provide their login credentials to anybody else, including family members.

3. All Users are connected to the Village's internal network via remote access must use up-to-date anti-virus and anti-malware software.

4. It is the User's responsibility to ensure that the remote access connection is given the same consideration as the User's internal System connection.

5. Internet access through the remote access connection shall be limited to Village business only, as described in herein.

6. All tablets issued by the Village will be remotely managed by IS for security purposes in the event the Tablets are lost, stolen, or compromised by an unauthorized user.

IX. ELECTRONIC DATA BACKUP

A. PURPOSE

To establish guidelines to prevent the loss of electronic data in the event of equipment failure or destruction; and provide the Village a reasonable means of indexing data for retrieval.

B. GUIDELINES

1. The guidelines for Electronic Data Backup shall include all data stored on Windows Servers and certain Windows electronic devices as defined periodically by the MIS.

2. All data files, user files, and E-Mail are eligible for back-up.

3. The Information Systems Division is not responsible for user data stored on desktop computers. All data shall be stored on the servers.

4. The Finance Department shall be responsible for data backup of the "Sungard Pentamation Public Sector" server.

5. All Village servers and User files shall be backed up in accordance with an applicable best practices schedule.