Acceptable Use Policy

for

Electronic Information Systems *and* Network Services

City of Somerville, Massachusetts

Joseph Curtatone, Mayor

Bruce M. Desmond, Chief Information Officer

This page intentionally left blank

Table of Contents

I. Acceptable Use

The electronic communication systems are the property of the City and all communications composed, sent, or received, are the property of the City.

As an authorized City of Somerville user of computing and electronic resources, you are not allowed to enable unauthorized users to access the network by using a City computer or a personal computer that is connected to the City network.

Employees should not consider any voice mail message, fax transmission, e-mail message, text message or Internet posting to be personal or confidential even if those messages, texts and postings were created, sent or received on a personal device not owned by the city but was allowed access to the City of Somerville network. Further, the use of passwords for security does not imply confidentiality. All passwords are the property of the City.

Electronic communications may be discoverable with or without notice, notwithstanding any password, nor if messages have been deleted. Subject to certain exceptions in the law, electronic communications may also be considered public records.

City of Somerville users of electronic communication systems and network services must adhere to the criteria listed below:

A. Scope

The computing and telecommunication resources at the City of Somerville support the educational, instructional, research, and administrative activities of the City of Somerville. The use of these resources is a privilege that is extended to employees of the City. As a user of these services and facilities, you have access to valuable City of Somerville resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

This document establishes specific requirements for the use of all computing and network resources at the City of Somerville. While every effort is made to insure the privacy of the City of Somerville user accounts, this may not always be possible. In addition, since employees are granted use of electronic information systems and network services to conduct City of Somerville business, there may be instances when the City of Somerville, based on approval from authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user.

In general, **acceptable use means respecting the rights of other computer users, other people, the integrity of the physical facilities and all pertinent license and contractual agreements.** If an individual is found to be in violation of the Acceptable Use Policy, the City of Somerville will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including

suspension or termination from employment with the City of Somerville. Individuals are also subject to federal, state and local laws governing the many interactions that occur on the Internet including the Massachusetts State Code of Ethics. These policies and laws are subject to change as state and federal laws develop and change.

1. This policy applies to all users of computing resources owned or managed by The City of Somerville. Individuals covered by the policy include (but are not limited to) city employees and staff, students, guests or agents of the administration, external individuals and organizations accessing network services via the city's computing facilities.

2. Computing resources include all City of Somerville owned, licensed, or managed hardware and software, and use of the City of Somerville network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

3. These policies apply to technology administered in individual departments, the resources administered by central administrative departments (such as the City of Somerville Libraries and Information Technology Services), personally owned computers and devices connected by wire or wireless to the city network, and to off-site computers that connect remotely to the City of Somerville's network services regardless of the ownership of the computer or device connected to the network.

B. **Personal Rights and Responsibilities:**

1. As an employee or staff person of the City of Somerville, the City of Somerville provides you with the use of work-related tools, including access to certain computer systems, servers, software and databases, telephone and voice mail systems, the Internet and e-mail systems whether owned by the City of Somerville or a vendor under contract with the City of Somerville.

2. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a City of Somerville employee or a person associated with the city via contractual agreement), and of protection from abuse and intrusion by others sharing these resources

3. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

4. You are responsible for knowing the regulations and policies of the City of Somerville that apply to appropriate use of the City of Somerville's technologies and resources.

5. You are responsible for exercising good judgment in the use of the City of Somerville's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

6. As a representative of the City of Somerville, you are expected to respect the City of Somerville's good name and reputation in your electronic dealings with everyone, both inside and outside the City of Somerville.

7. All users of the City of Somerville's network and computing resources are expected to respect the privacy and personal rights of others. Do not access or copy another user's email, data, programs, or other files without the written permission of the City's Chief Information Officer or his designee, who are bound to the procedures outlined in Sect. IV. Emergency Access to Accounts and Information

8. Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could subject you to disciplinary actions by the City of Somerville as well as legal action by those who are the recipient of these actions.

9. While the City of Somerville does not generally monitor or limit content of information transmitted on the City network, it reserves the right to access and review such information under certain conditions. These include, but are not necessarily limited to:

    1. Investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that City is not subject to claims of institutional misconduct.

2. External law enforcement agencies and City Public Safety agencies may request access to files through valid subpoenas and other legally binding requests. All such requests must be approved by the City Solicitor. Information obtained in this manner can be admissible in legal proceedings or in a City of Somerville hearing.

10. You are individually responsible for the appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware.

11. As an authorized City of Somerville user of computing and electronic resources, **you are not allowed** to enable unauthorized users to access the network by using a City computer or a personal computer that is connected to the City network.

12. The City of Somerville is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.

13. You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access.
    1. One example of a "reasonable effort" is not walking away from a workstation when you remain logged into the City system

14. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing the City's network and computing resources.

15. You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

16. You may use only the computers, computer accounts, and computer files for which you have authorization.
    1. Access to files or information that you are not authorized to access and which reside on City of Somerville equipment (owned, leased or contracted) can only be approved by specific personnel when there is a valid reason to access those files or information. Authority to access files or information outside of your normal authorization can only come from the City Solicitor, the Director of Personnel or the Chief Information Officer in conjunction with requests and/or approvals from Executive staff members and/or department heads of the City of Somerville, as outlined in Sect. IV Emergency Access to Accounts and Information.

17. You may not use another individual's account, or attempt to capture or guess other users' passwords.

18. You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

19. You must not use City computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

20. Do not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) on the City of Somerville network and/or computing systems, unless you have been specifically authorized to do so by the City of Somerville Information Technology Group.

21. Never perform or participate in activities of any kind that would jeopardize the City of Somerville's good standing with associated groups/organizations.

22. Do Not use of the City's computing services and facilities for political purposes.

23. Do Not use of the City's computing services and facilities for personal economic gain

C. Fair Share of Resources

1. The Information Technology Department and other City of Somerville departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The City of Somerville network, computer clusters, mail servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the City is explicitly forbidden.

2. The City of Somerville may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

D. Adherence with Federal, State, and Local Laws

1. As an employee or staff member of the City of Somerville, you are expected to uphold all local ordinances as well as all state and federal laws. Some City guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property. As a user of the City's computing and network resources you must:
    1. Abide by all federal, state, and local laws.
    2. Abide by all applicable copyright laws and licenses. The City of Somerville has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.
    3. Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.
    4. Never use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.
    5. Abide by the Code of Ethics as outlined by the Commonwealth of Massachusetts

II. Passwords

This section describes the City of Somerville requirements for acceptable password selection and maintenance to maximize security of passwords and minimize the misuse or theft of passwords. Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs and the activity of malicious hackers and spammers, passwords are very often the weakest link in securing data. All passwords (e.g., email, web, desktop computer, etc.) should be strong passwords and follow the standards listed below. In general, a password's strength will increase with length, complexity and frequency of changes. Greater risks require a heightened level of protection. Stronger passwords augmented with alternate security measures such as multi-factor authentication, should be used in such situations. High risk systems include but are not limited to: systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure. System administrators are expected to set a good example through a consistent practice of sound security procedures.

A. All passwords must meet the following minimum standards, except where technically infeasible.

1. ***MUST*** be at least eight alphanumeric characters long
2. ***MUST*** contain at least one digit or punctuation character as well as letters (e.g., 0-9, ~'!@#$%()_-'{.})
3. ***MUST*** contain both upper and lower case characters (e.g., a-z, A-Z)
4. ***MUST NOT*** be solely based on easily guessed personal information, such as names of family members, pets, etc.
5. **MUST NEVER** use personal or fiscally useful information such as Social Security or credit card numbers as a user ID or a password
6. **MUST NEVER** be written down or stored on-line unless adequately secured. All passwords are to be treated as sensitive information and should therefore never be written down.
7. **MUST NEVER** use the password storage feature offered on Windows or other operating systems. *This feature creates a password file that is vulnerable to hackers.*
8. **MUST NEVER** insert Passwords into email messages or other forms of electronic communication without the consent of the Information Technology Department (IT)
9. **MUST** encrypt Passwords that could be used to access sensitive information when in transit
10. **MUST NEVER** use the same password for your access needs external to City of Somerville systems (e.g., online banking, benefits, etc.)
11. **MUST** change Passwords at least every six months
12. **MUST NEVER** share individual passwords with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent of IT and must have a responsible primary contact person. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those passwords and that person must ensure that only appropriately authorized employees have access to the passwords.
13. **MUST** change a password immediately if it is suspected to have been compromised, it should also be reported to IT.
14. Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.
15. **Note:** The following special characters **cannot be used** in passwords for City of Somerville systems: *+,/:;<=>?[\]|^&

III. Electronic Communication

The City of Somerville recognizes the importance of technology for access to information and to enable communication that enhances the City's efforts to provide its citizens the best and most efficient services. Accordingly, the City provides designated staff with the technology to communicate verbally, send electronic messages and information via radios, telephones, cell phones, voice mail, fax machines, electronic mail, and the Internet. It is the City's policy that use of these systems and devices is subject to the same management oversight as any other employee activity.

A. The electronic communication systems are the property of the City and all communications composed, sent, or received, are the property of the City.

B. City of Somerville electronic information systems and network services should only be used for appropriate business purposes of the City of Somerville. Failure to observe this policy could result in the loss of the privilege for the individual and others in the organization and may subject individuals to disciplinary action, up to and including termination of employment.

C. The City reserves the right to retrieve, read or otherwise access any electronic communication messages or other data stored on City owned or contracted equipment and on any personal device on the city network not owned by the City of Somerville for any purpose and without limitation including systems maintenance and compliance monitoring.

D. Employees should not consider any voice mail message, fax transmission, e-mail message, text message or Internet posting to be personal or confidential even if those messages, texts and postings were created, sent or received on a personal device not owned by the city but was allowed access to the City of Somerville network. Further, the use of passwords for security does not imply confidentiality. All passwords are the property of the City.

E. Electronic communications may be discoverable with or without notice, notwithstanding any password, nor if messages have been deleted. Subject to certain exceptions in the law, electronic communications may also be considered public records.

F. City of Somerville users of electronic communication systems and network services must adhere to the criteria listed below:

1. The electronic communication systems and network services should not be used for any illegal activity, including but not limited to the transmission of copyrighted or trade secret material, proprietary financial information, or similar materials, without prior management authorization in writing. The transmission of obscene, defamatory, or threatening material or the propagation of any type of criminal activity is strictly prohibited.

2. Data and messages directed to one or more employees or officials should be treated as confidential by other employees and should only be accessed by the intended recipient. Employees are not authorized to retrieve or read any messages or data that are not sent to them unless the intended recipient gives express permission. Also, employees should not use a code, access a file, or retrieve any stored information unless authorized to do so.

3. The electronic communication systems and network services should not be used to create any offensive or disruptive messages or images. Among those which are considered offensive are any messages or images which contain sexual implications, racial slurs, gender-specific comments, or any other comment which might constitute intimidation, hostile or offensive material based on one's sex, race, color, national origin, age, religion, sexual orientation or physical or mental disability. Employees must not use the Internet to access pornographic, sexually oriented, or otherwise offensive or inappropriate websites.

4. Electronic communication users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of the City unless expressly authorized to do so. Neither should they construct a communication so it appears to be from someone else (false identity).

5. Executable programs imported from other sites to City computers must not be imported or used unless the Information Technology Department (IT) has authorized them. Once authorized, they must first be subject to virus detection procedures approved by IT. Private e-mail and web sites accounts are not permitted on City computer systems.

6. Upon request of a Department Head and with the approval of the Mayor, monitoring of electronic communication systems and network services usage can and will be implemented to review employee productivity, investigate claims of criminal activity or violations of this policy as well as other legitimate business reasons.

7. The City's electronic communication systems shall not be used for commercial promotion, product endorsement or political lobbying. However, political lobbying or other activities that may be deemed to be political in nature shall be permitted to the extent that such activities are a part of the official responsibilities of an employee, provided that such activities relate to political issues rather than directly relating to specific political candidates.

8. The electronic communication systems and network services should not be used for personal activities such as games, entertainment, and correspondence. Department Heads should resolve any questions regarding the professional relevance of the use of Electronic Information Systems and Network Services including the content of websites and email.

9. Electronic communication systems and network services that incur per-use fees, such as cellular telephones and their radio function, should be used for necessary work related purposes only. Whenever possible, less expensive communications devices, such as land-line telephones or electronic mail, should be used.

10. Employees may be asked to reimburse the City for costs associated with inappropriate or personal use.

11. Land line telephones will be installed with the capability for local calling. If long distance capabilities are required it must be requested in writing by the department head.

IV. Access to Accounts and Information (Emergency or Otherwise)

The City of Somerville offers electronic services to its computer users to perform work for the City of Somerville in support of its mission. While the City of Somerville does not generally monitor or limit content of information transmitted on the City network, the City reserves the right to retrieve, read or otherwise access any electronic communications messages or other data stored on City owned equipment or on equipment owned by third party vendors under contract with the City of Somerville for any purpose without limitation including systems maintenance and compliance monitoring. Employees should not consider voice mail, fax mail, e-mail messages, text messages or Internet postings to be personal or confidential. Further, the use of passwords for security does not imply confidentiality. All passwords are the property of the City. Electronic communications may be discoverable with or without notice, notwithstanding any password, even though messages may have been deleted. Subject to certain exceptions in the law, electronic communications may also be considered public records.

A. Data and messages directed to one or more employees or officials should be treated as confidential by other employees and should only be accessed by the intended recipient. Employees are not authorized to retrieve or read any messages or data that are not sent to them unless the intended recipient gives express permission. Also, employees should not use a code, access a file, or retrieve any stored information unless authorized to do so.

B. While efforts are made to ensure reasonable expectations of privacy for computer users, legitimate reasons will arise that require access to information held on the City of Somerville workstations, servers or peripherals and on servers owned by third party vendors under contract with the City of Somerville. These exceptions may be required based on legal action (such as a court order or Freedom of Information Act), may involve the health and/or safety of an individual or group, or be prompted by urgent City of Somerville business needs. Should an individual user be unavailable or unable to provide permission to access it, and if circumstances supersede the right to privacy, access without the owner's permission will be provided with the approval of an authorized City of Somerville official as described in the following procedures.

C. Procedure for accessing an employee's E-Mail or data stored on City of Somerville equipment or equipment owned by a third party vendor under contract with the City of Somerville.

1. The department head will contact the Chief Information Officer with the name of the person who requires access, the reason access is required, the name of the employee whose existing information is to be accessed or exported, and specifics as to what information is needed. If the request is for email messages, the requestor must specify exactly what information is being requested.

2. The Chief Information Officer will seek guidance and approval from the City Solicitor and the Director of Personnel (or during their absence their deputy).

3. If approved, the Chief Information Officer talks directly to the appropriate IT technician who will comply with the request. The IT technician either exports the data or requested information to a portable storage device and delivers it to the City Solicitor or provides the City Solicitor access to the requested information for their review. **The technician will only release requested information to the City Solicitor.**

D. Emergency information access due to urgent City of Somerville business

When business needs require access to employee electronic information – whether stored in a personal mailbox, personal network space, on a personal hard drive, file backups or equipment owned by third party vendors under contract with the City of Somerville and the information caretaker is unavailable, the department head should contact the Chief Information Officer (or designee), who will review the request and either authorize the specific access as necessary or deny the request. Examples of an employee's inability to provide consent include, but are not limited to the following:

1. Administrative leave

2. An employee leaves unexpectedly and ends up on a prolonged absence

3. An employee is terminated

4. An employee is incapacitated or is otherwise unavailable and emergency access is required

E. Documentation

The Chief Information Officer will follow direction from the City Solicitor and the City Archivist regarding the preservation and archival of requested data, and will document the request, disclosure details, the name and title of the requestor, and the reason(s) for the emergency request.

F. Out of Office message

1. When an employee is unavailable to receive and respond to email and urgent business needs require continuity of communication, the employee's department head may request that an "Out of Office" message be placed on the employee's email account.

2. Procedure for creating an "Out of Office" message for an Unavailable Employee's Email Account

   1. The requestor's department head must contact the Chief Information Officer and provide details of the request including; the name of the email account owner who needs the Out of Office message added to their mailbox, and the text of that message and how long the out of office message should remain in place.
   The Chief Information Officer receives the department head request and works with Information Technology staff to comply with the request in a timely fashion.

G. Information access (emergency or otherwise) in response to a court order, Public Records Act or other compulsory legal process

1. Any request for access to electronic information from the City of Somerville in the form of a public records request or other legal action must be immediately forwarded to the City Solicitor. The City of Somerville's legal representatives will guide any further actions by City of Somerville employees.

2. Any electronic information collected per a Public Records Act request or other legal action or other compulsory legal process **will only be released to the City Solicitor and never directly to the requestor.**

3. Investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of City policy, or as may be necessary, to ensure that the City is not subject to claims of institutional misconduct.

V. Personally Owned Devices

This policy forms part of the city governance framework for acceptable use. It is particularly relevant to anyone who uses Personally Owned Devices for work purposes. This policy applies to all employees, full time staff, part time staff, students, interns, volunteers and third parties acting in a similar capacity to our employees.

A. Definitions

1. **Personally Owned Device:** In contrast to Information Technology (IT) devices owned by the City of Somerville, Personally Owned Devices (PODs) are any electronic (IT) devices owned by a person or entity other than the City of Somerville.

2. **Typical PODs include but are not limited to:** laptops, tablet computers, ultra-mobile PCs (UMPCs), desktop PCs, Personal Digital Assistants (PDAs), palmtops, cellphones, smartphones, digital cameras, digital memo recorders, printers, and for the purposes of this policy includes portable storage media such as USB memory sticks, memory cards, portable hard drives, floppy disks etc.

3. **Work Purposes:** Making and receiving work related phone calls and text messages, accessing, reading and/or responding to work emails, accessing City of Somerville data via non City of Somerville equipment while working in a home-office environment or simply accessing City of Somerville data via non City of Somerville equipment to perform an authorized City of Somerville job function regardless of where you are situated are some examples of using PODs for work purposes.

B. Policy

1. Individuals who wish to opt-in to POD use on the City of Somerville network must be authorized by the Information Technology Department and must explicitly accept the requirements laid out in this policy.
2. The City of Somerville reserves the right to **not authorize** individuals, or to **withdraw** authorization, if the city deems an individual's use of PODs not to be appropriate and/or in the best interests of the City of Somerville.
3. The City of Somerville will continue to provide its choice of fully owned and managed IT devices as necessary for work purposes, eliminating any compulsion for anyone to opt-in to use PODs if they choose not to do so.
4. The City of Somerville and the owners and users of PODs share responsibilities for information security.
5. Nothing in this policy affects the City of Somerville's ownership of city information, including all work-related intellectual property created in the course of work on PODs.
6. City data can only be created, processed, stored and communicated on personal devices running the City of Somerville's chosen Mobile Device Management (MDM) client software and antivirus software.
7. The City of Somerville is not responsible for replacing POD's if lost broken or damaged
8. Devices not running approved MDM client software and approved antivirus software (including devices that cannot run MDM client software and antivirus software, and devices on which the owners decline to allow IT to install MDM client software and antivirus software with the rights and privileges it needs to operate appropriately, and devices on which MDM client software and antivirus software is disabled or deleted after installation) are not and will not be granted access to the city network and they must not be used to create, modify, store or communicate city data.
9. POD users must use appropriate forms of user authentication approved by Information security, such as user IDs, passwords and authentication devices.
10. The City of Somerville has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete city data without reference to the owner or user of the POD.
11. The City of Somerville has the right to seize and forensically examine any POD believed to contain, or to have contained, city data where necessary for investigatory or control purposes.
12. POD users must ensure that valuable city data created or modified on PODs is backed up regularly, preferably by connecting to the city network and synchronizing the data between POD and a network drive, otherwise on removable media stored securely.
13. Any POD used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN) and while stored on the POD or on separate storage media (e.g. using True Crypt), whatever storage technology is used (e.g. hard disk, solid-state disk, CD/DVD, USB/flash memory stick, floppy disk etc.).
14. The City of Somerville and the Somerville IT department are not responsible for supporting the functionality or operation of any POD. PODs used will receive limited support from IT on a 'best effort' basis for business purposes only.
15. While employees have a reasonable expectation of privacy over their personal information on their own equipment the City of Somerville's right to control its data and manage PODs may occasionally result in support personnel unintentionally gaining access to their personal information.

16. Information security incidents affecting PODs used on the City of Somerville network should be reported immediately to the IT Help/Service Desk.
17. Internal Auditing is authorized to assess compliance with this and other city policies at any time.
18. All employees are responsible for complying with this and other city policies at all times.
19. The agreement comes with conditions, including that users allow the City of Somerville to install a public key infrastructure (PKI) device certificate on the devices for authentication whenever they're used to access the network.
20. Remote-wipe software maintained by the City of Somerville must also be installed on the device.

C. User Compliance

1. Per this agreement, users acknowledge that they understand that the device and the user are subject to the same responsibilities, procedures and enforcement as devices that are owned and maintained by the City of Somerville. Furthermore, users acknowledge that personal devices can be seized for an indeterminate amount of time if it, or the data on it, is part of a legal dispute.

2. When you use City of Somerville computing services, and accept any City of Somerville issued computing or telecommunication device, you agree to comply with this and all other computing related policies. You have the responsibility to keep up-to-date on changes in the computing environment, as published, using City of Somerville electronic and print publication mechanisms, and to adapt to those changes as necessary.

VI. Safe Email Practices

Emails are one of the most popular modes of virus distribution these days, so to keep your computer healthy, and help prevent spreading viruses you need to practice a few safety rules to minimize the chance of you sending a virus to someone else. Remember, if your computer is infected, you can infect someone else. This is a case where good citizenship is important. Safe email practices are important; they minimize the chance of your pc getting a virus.

A. Safety Rules

1. Attachments

1. Attachments require special attention. They could contain viruses – even if it's coming from the computer of a friend. Therefore: Never open attachments if you don't know who they're from.
2. If you do know who it's from but the subject line sounds suspicious, contact your friend before opening.

B. Spoofing (Spoofing is masquerading as someone else)

1. Viruses often "spoof" the “from” address usually getting the name from an infected computer's address book. The infected computer could be a friend's which is why all email - even from friends should be held suspect.

C. Tempting / Flattering Subject lines

1. Viruses also try to come up with a compelling subject line to get you to open them. If the subject or attachment seems strange, too urgent, too alarming, too good to be true, then it probably is. Don’t open it. As soon as you open it it’s too late.

D. Turn Off Preview Pane

1. The preview feature of Email programs like Outlook can allow you to unwittingly execute the code in an infected email. Therefore:
   1. Turn off the preview Pane in Outlook: Go to Menu > View > Layout... in Outlook and uncheck the box for "Show preview pane".

E. Beware of strange messages

1. Examine your list of unopened messages carefully before you open any of them.
2. If you didn't expect a message, if you don't know the sender, if the subject or attachment seem strange, too urgent, too alarming, too good to be true, or the sender and the subject don't jibe, just delete the message, along with any attachments, without opening it.

F. Don't be fooled by Dirty Tricks

1. Most computer worms (a kind of malicious program) spread themselves via email by spoofing addresses found in the infected computer's address book and sending copies of itself to other addresses in the address book, so it's very likely that an infected message can appear to come from someone you know. Many of these messages will use vague or generic subject lines like "Re: " or "Hi." Others will try to look like they come from a technical support service, or even from Microsoft. Be careful about opening these.

G. Use Antivirus software, and keep it updated: This will help protect your machine and the machines of others on the internet if a virus should happen to get through to your machine.

H. Don't Unsubscribe: Spammers often include an "unsubscribe from this list" link in their messages. This makes them appear more responsible and reputable, but they often use this as a way to confirm your email address so they can send you more spam or sell your email address to other spammers. If you don't want it, mark it as junk and delete it.

I. Be a Good Internet Citizen.

1. Don't use your email in ways that will contribute to the problem.
2. Don't send unsolicited email and attachments.
3. Don't forward chain letters.
4. Don't respond to or participate in email hoaxes.
5. Don't send attachments which use the "unsafe" file types.

VII. ENFORCEMENT

A. The use of the City's Electronic Information Systems and Network Services constitutes employee consent to monitoring of the systems and is conditioned upon strict adherence to this policy. Any employee who violates this policy or uses the City's Electronic Information Systems and Network Services for improper purposes may be subject to discipline, up to and including discharge.

B. Department Heads and supervisors are responsible for ensuring that all of their employees using the City's Electronic Information Systems and Network Services have read this policy and understand its applicability to their activities. This policy is not intended to replace day to day administrative procedures specific to each department's operational needs.

C. The electronic communication systems are the property of the City and all communications composed, sent, or received, are the property of the City. Employees should not consider any voice mail message, fax transmission, e-mail message, text message or Internet posting to be personal or confidential even if those messages, texts and postings were created, sent or received on a personal device not owned by the city but was allowed access to the City of Somerville network. Further, the use of passwords for security does not imply confidentiality. All passwords are the property of the City.

D. **Electronic communications may be discoverable with or without notice, notwithstanding any password, nor if messages have been deleted. Subject to certain exceptions in the law, electronic communications may also be considered public records.**

By signing this document you acknowledge you have read the document and agree to abide by the terms and conditions of the City of Somerville's Acceptable Use Policy.

Signature: _____

Print Name: _____ **Date:** _____

Effective Date: July 1, 2015
Last Reviewed: April 21, 2015
Next Scheduled Review: April 21, 2016