
# City of Springfield

*Policy for the Use of*
*Information Technology Resources*

Revised
March 3, 2016

## *I. Purpose*

The City provides Information Technology Resources to employees at City expense for their use in performing their duties for the City. This material sets forth the City's policy for proper use of Information Technology Resources. This policy also sets forth the City's policy regarding when Information Technology Resources used by an employee may be accessed by Directors, managers, and supervisors, and when data or other information obtained through Information Technology Resources may be disclosed to third parties. This policy also sets forth guidelines for securing data and addresses confidentiality issues.

This policy can be viewed at any time by logging on the City of Springfield's Intranet site. Any changes or updates to this policy will be delivered to all users of the City Network via electronic or other means. No manager or supervisor has the authority to alter or amend this policy.

## *II. Definitions*

"Information Technology Resources" means the City's computers, software, electronic mail (email), internet systems, intranet systems, USB storage devices, photocopying equipment and telecommunications systems including telephones, speakerphones, voice mail, fax machines, Virtual Private Networks (VPN), cell phones, camera phones, and pagers, and also means personal equipment when attached to the City Network or other City-owned systems. "Information Technology Resources" also includes all devices (e.g., personal computers, laptops, email-enabled cellular phones, PDA's, etc.) that connect to the City Network through a wireless communication mechanism, including any form of device capable of receiving and transmitting packet data over a wireless network.

"City" means the City of Springfield, Illinois, a municipal corporation.

"City Network" or "Network" includes the City of Springfield's Network and City Water, Light & Power's Network.

"Director" means the director of the appointed offices identified in Section 32.05 of the 1988 Code of Ordinances of the City of Springfield, as amended. Unless otherwise specified, "Director" means the employee's Director as the case may be.

"ISD" means the Information Systems Division of the Office of Public Utilities.

"Public Record" means, as defined in the Local Records Act, 50 ILCS 205/3, any book, paper, map, photograph, digitized electronic material, or other official documentary material regardless of physical form or characteristics, made, produced, executed or received by the City pursuant to the law or in connection with the transaction of public business and preserved or appropriate for preservation by the City as evidence of the City's organization, function, policies, decisions, procedures, operations or other activities or because of the informational data contained therein. Email messages that do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt are generally not "Public Records." Rather, they are informal communications that are similar to communications during telephone conversations or conversation in an office hallway and are generally short-lived, with no historical significance or public importance.

## *III. Applicability/Eligibility*

This policy applies to all City employees, contractors, volunteers and other individuals (hereinafter "employees") who are provided direct access to Information Technology Resources and who are employed by offices under the jurisdiction of the Mayor. Additionally, all City contracts shall contain adequate terms and conditions necessary to ensure that all contractors, vendors, or other third parties that have access to Information Technology Resources or to any data or information obtained through them are bound by the terms of this policy. Such contracts shall further provide that contractors, vendors, or other third parties may not share information obtained through Information Technology Resources without the express written consent of an authorized City official. Employees shall consult with ISD and the Office of Corporation Counsel to ensure compliance.

Personal equipment will be governed by this policy when attached to the City Network or any other systems owned by the City.

Directors, managers, and/or supervisors, or their designees shall request approval of employee Network and Internet access from the ISD by completing the Network Security Request Form (Attachment A) which may be obtained at the City's Intranet home page. This capability will be provided on an as-needed basis and is a revocable privilege. ISD shall make recommendations to the Mayor, Director, manager, and/or supervisor regarding use and misuse of these systems and the continuation of such services to individual employees. Upon the termination or transfer of an employee, the Director, manager, or supervisor must notify ISD to request removal of access to the City Network and all applications.

## *IV. General Policy*

### *A. Ownership*

All Information Technology Resources, and all other work place electronic systems, hardware, software, temporary or permanent files and any related systems or devices used in the transmission, receipt or storage of information are the property of the City. Email messages are considered City property and when stored and backed up on the City Network may be retrieved from storage even though they have been deleted by the sender and receiver. These messages may be used in disciplinary proceedings. Because all workplace electronic systems are the property of the City,

employees may not add hardware or software to any related systems or devices without the approval of their Director and ISD.

*B. Uses of Resources*

It is City policy that Information Technology Resources, like other City assets, are to be used for the benefit of the City. Use of Information Technology Resources to violate other City policies, software licenses, copyrights, or any other federal, state, or applicable international law is prohibited and may lead to disciplinary action, up to and including discharge. All employees who use Information Technology Resources shall certify that they have read and fully understand the contents of this policy.

Any loss of information must be reported immediately to ISD and the Director. All City-owned data files that will reside on computers outside the City's facilities or data centers and that contain confidential information must be encrypted (please see Exhibit B. File Encryption Procedures) and password protected. Employees must immediately report any breach or potential breach of security that may compromise confidential information or data to the Director and ISD.

Employees should be aware that many electronic documents and communications may be subject to disclosure under the Freedom of Information Act. A broader range of documents may be subject to disclosure in response to a subpoena issued as part of a lawsuit or a criminal investigation. Employees must treat electronic documents and communications with the same level of care, both in production and storage, as are accorded documents and communications that are in print form.

City employees not familiar with certain software products, the Internet, or using their email account are strongly encouraged to attend classes prior to their use.

*C. Personal Use*

Information Technology Resources must be used for official City business only, with allowance made for reasonable personal use that does not otherwise violate this policy. Personal use will be considered reasonable if it meets the following criteria: (1) it does not adversely affect the employee's performance or official duties, (2) it is of minimal duration and frequency, (3) it does not violate any other employment policy or rule, or any federal, state or local law or regulation. Should employees make incidental use of Information Technology Resources to transmit personal messages, such messages will be treated no differently than other messages and may be accessed, reviewed, copied, deleted, or disclosed. Any message may be disclosed to, or read by, others beyond its original intended recipients.

All files, documents, emails, etc. must be protected by storing the data on drives other than the computer's C: drive so that the information may be backed up and restored if needed.

*D. Unacceptable Uses*

Improper use of Information Technology Resources is strictly prohibited. Actions that constitute unacceptable uses even if not specifically addressed elsewhere in this policy include, but are not limited to:

- Using Information Technology Resources for, or in support of, any illegal purpose.
- Using Information Technology Resources for, or in support of, any obscene or pornographic purposes including, but not limited to, the retrieving or viewing of any sexually explicit material. If an employee inadvertently accesses such information, he or she should immediately disclose the inadvertent access to a superior and contact ISD to have the site blocked. This may protect the employee against allegations of intentionally violating this policy.

- Using Information Technology Resources for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass, threaten, or "stalk" another individual.
- Using Information Technology Resources to upload, post, email, transmit, or otherwise make available any content that is unlawful, dangerous, or may cause a security risk.
- Knowingly making a false, misleading, or unauthorized statement of City policy, either expressly or by implication.
- Using Internet games or tools such as discussion boards, chat rooms, and instant messaging for personal rather than City business purposes.
- Using profanity, obscenity, or language that is generally considered offensive or threatening to persons of a particular race, color, gender, religion, national origin, ancestry, age, sex, sexual orientation, or to persons with disabilities as those terms are defined in Chapter 93 of the 1988 City of Springfield Code of Ordinances, as amended.
- Knowingly using copyrighted materials, including commercial software, without permission of the copyright holder, and/or in violation of state, federal, or international copyright laws. (If employees are unsure whether they are using materials in violation of copyright provisions, they should contact the Office of Corporation Counsel.)
- Knowingly violating any federal or state statutes or any City policies and/or procedures regarding the protection of privacy or confidential information.
- Using the Information Technology Resources for personal financial gain or commercial activity.

*E. Inspections*

***The City reserves the right to access, audit, block, delete, disclose, intercept, monitor, publish, recover, restrict, restore, review, screen, or trace any data or information stored on the City's Information Technology Resources at any time without notice.***

Supervisors, with the written approval of the Director, have the authority to inspect the contents of any equipment, files, calendars or electronic mail of their subordinates in the normal course of their supervisory responsibilities. After obtaining written approval from the Director, ISD shall extract stored email messages or other pertinent information as required, when requested to do so by an authorized supervisor. Reasons for review include, but are not limited to, system hardware or software problems, Spyware, viruses, or other intrusive entities, general system failure, regular system maintenance, a lawsuit against the City, freedom of information request, suspicion of a crime or violation of policy, or a need to perform work or provide a service when the employee is unavailable.

*F. No Expectation of Privacy*

Messages created, stored, transmitted or received via Information Technology Resources may be read by others for a variety of valid reasons. Although this statement is also true of many other types of City correspondence, the nature of an email, instant message or faxed message can lead one to forget or ignore the fact that the message cannot be considered to be the private property of the sender or recipient even though passwords or encryption codes are used for security reasons. As with all Information Technology Resources, these messages are subject to all provisions of this policy. Employees expressly waive any right of personal privacy or expectation of personal privacy in anything they create, store, send, or receive on or through Information Technology Resources.

Use of passwords to gain access to Information Technology Resources or to encode particular files or messages does not imply that employees have an expectation of personal privacy in the material they create, receive, transmit, or store on any system or expectation of confidentially for any information.

*G. Confidential Information*

The law requires that all employees protect the integrity of the City's confidential information as well as the confidentiality of others. In the performance of their duties and through their use of Information Technology Resources, employees may have access to confidential information. No employee shall disclose confidential information to anyone, including another City employee, except in the course of official City business. Confidential information should never be transmitted or forwarded to other City employees who do not need to know the information. Unauthorized or improper disclosure of confidential information and use of Information Technology Resources to communicate or otherwise disclose confidential information is prohibited and may lead to disciplinary action, up to and including discharge.

Information such as Social Security Numbers and other personal information shall not be transmitted without written permission from the Director. Individuals who have access to this information shall read and understand this policy; especially as it relates to security and confidentiality. Employees who have access to confidential information may not forward the information to third-parties without written permission of the Director. Employees are also responsible for the confidentiality of passwords assigned to computer data. Divulging passwords may lead to disciplinary action.

If you are unsure whether information is confidential, consult the Office of Corporation Counsel. Some types of information which can be confidential include, but are not limited to:

- Personnel information;
- Any social security number;
- Personal information about other employees, such as home addresses and phone numbers;
- Information relating to litigation or administrative hearings of a criminal or civil nature;
- Information which, if released, would give a competitive advantage to one competitor or bidder over another;
- Information related to location or price of property the City might buy;
- A draft or working paper involved in the preparation of proposed legislation;
- Trade secrets, commercial or financial information of outside businesses;
- Personal family information of another City employee;
- Certain information the City obtains from businesses;
- Health records;
- Information about customers, credit histories, draft reports, initial recommendations;
- Certain tax information.

*H. Disclaimer*

The City uses filtering software to screen Internet sites for offensive material. The Internet is a collection of thousands of worldwide networks and organizations that contain millions of pages of information. Employees are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content; Nudity; Sex; Gambling; Violence; Weapons; Hacking; Personals/Dating; Lingerie/Swimsuit; Racism/Hate; Tasteless; and Illegal/Questionable. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an email address on the Internet may lead to receipt of unsolicited email containing offensive content. If an employee inadvertently accesses such information, he or she should immediately disclose the inadvertent access to a supervisor and contact ISD. This may protect the employee against allegations of intentionally violating this policy.

Employees accessing the Internet do so at their own risk. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful and employees gain access to inappropriate and/or harmful material, **the City will not be liable**. To minimize these risks, employees' use of the City Network is governed by this policy.

*I. Unauthorized Access and Security*

All employees are to report promptly all suspected intrusions into Information Technology Resources by unauthorized persons and any breaches of security violations of acceptable use and the transmission of web addresses or email information containing inappropriate material (as outlined elsewhere in this policy) to the Director or the Manager of ISD. Failure to report any incident promptly may subject the employee to corrective action consistent with the City's employment policies. In order to maintain the security of the City Network, employees are prohibited from engaging in the following actions:

- Knowingly disrupting the use of the City Network for other users, including, but not limited to, disruptive use of any processes or programs, sharing logins and passwords or utilizing tools for ascertaining passwords, or engaging in unauthorized or unlawful entry into an electronic system to gain information (i.e. "hacking").
- Knowingly spreading computer viruses or programs that loop repeatedly, infiltrating a computer system without authorization, or damaging or altering without authorization the software components of a computer or computer system.
- Disclosing the contents or existence of the City Network, confidential information, email correspondence, or other information to anyone other than authorized recipients.
- Sharing logins or password(s) and unauthorized information regarding other users' passwords or security systems.
- Downloading unauthorized games, programs, files, electronic media, and/or stand-alone applications from the Internet that may cause a threat to the City Network.

## *V. Email Policy Guidelines*

*A. Authorized Uses*

Email addresses are assigned to City employees to provide them with an efficient mechanism for conducting City business. As such, only correspondence relating to City business should be transmitted, with allowance made for reasonable personal use that does not otherwise violate this policy. Personal use will be considered reasonable if it meets the following criteria: (1) it does not adversely affect the employee's performance or official duties, (2) it is of minimal duration and frequency, (3) it does not violate any other employment policy or rule, or any federal, state or local law or regulation. Employees must use email in accordance with the General Policy set forth above. Communication by email is encouraged when it results in the most efficient or effective means of communication. The sender of email messages retains the primary responsibility for ensuring that the communication is received by the intended receiver.

*B. Uses Subject to Prior Approval*

The following uses require the prior written approval of the employee's Director:

1. Using hardware, related computer equipment and software not owned or purchased by the City to transmit email for City business purposes from a City office or facility. However, this does not prohibit an employee from using his or her own hardware or related computer equipment or software to transmit email to the City.
2. Read electronic mail of another employee without prior written approval. However, an employee's supervisor may inspect the contents of email pursuant to the section entitled "Ownership" in this policy.

*C. Prohibited Uses*

In addition to the Unacceptable Uses outlined in the General Policy above, the following actions are prohibited:

1. Intercepting, eavesdropping, recording, altering another person's email message.
2. Forwarding a prohibited message such as chain emails, etc.
3. Adopting the identity of another person on any email message, attempting to send electronic mail anonymously, or using another person's password; anonymous or pseudonymous electronic communications are prohibited.
4. Misrepresenting your affiliation on any email message.
5. Composing and sending email which contains racial or sexual slurs or jokes, or patently harassing, intimidating, abusive, or offensive material to or about others.
6. Using email for any commercial promotional purpose, including email messages offering to buy or sell goods or services.
7. Using email for political purposes or to conduct employee organization, association or union business except that Union stewards and/or officers may utilize email for the purpose of investigating or processing grievances if such transmission is primarily to expedite communication regarding such matters and is reasonable with respect to time and volume.
8. Sending or receiving any software in violation of copyright law.
9. **BROADCAST MESSAGES TO ALL NETWORK USERS ARE PROHIBITED WITHOUT THE PRIOR AUTHORIZATION OF THE SENDING EMPLOYEE'S DIRECTOR, OR THE OFFICE OF THE MAYOR, OR IF TO NOTIFY USERS OF ISSUES RELATING TO THE NETWORK OR POLICY CHANGES, THE ISD DIRECTOR**.
10. Furnishing passwords to others.

*D. Confidential Information*

In addition to the General Policy relating to confidential information for uses of all Information Technology Resources, including email, employees are directed to exercise an even greater degree of caution in transmitting confidential information on the email system because of the reduced effort required to redistribute such information. As stated in the General Policy, confidential information should never be transmitted or forwarded to other City employees who do not need to know the information. To reduce the chance that confidential information may inadvertently be sent to the wrong person, avoid misuse of distribution lists when sending information and make sure that any lists used are current. Review each name on any list or recipients before transmission to ensure that all recipients need to know the information. Examples of confidential information are set forth in the General Policy above. If you are unsure whether information is confidential, consult the Office of Corporation Counsel.

Email messages that contain confidential information should have a confidentiality legend in all capital letters as part of the message in a form similar to the following:

**"THE ABOVE MESSAGE, INCLUDING ANY ATTACHMENTS, IS INTENDED ONLY FOR THE USE OF THE ADDRESSEE AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL AND PROHIBITED FROM DISCLOSURE UNDER APPLICABLE LAW. YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU RECEIVE THIS E-MAIL IN ERROR, RETURN TO THE E-MAIL ADDRESS LISTED ABOVE."**

Email received from or by Corporation Counsel, his or her staff, or an attorney representing the City may also include this warning header on each page:

"*ATTORNEY-CLIENT PRIVILEGE; DO NOT FORWARD WITHOUT PERMISSION."*

Because copies of email may be placed on back-up or other systems an employee does not control and may, under certain circumstances, be accessed by ISD or others without a need to know the information, employees are reminded that email may be inappropriate to communicate certain types of confidential information. In addition, to minimize inadvertent disclosures, employees should not access their email messages for the first time in the presence of others. Messages should not be left visible on the monitor when a user is away from his or her computer. Passwords should be routinely changed as required by ISD.

*E. Copyright Infringement*

The ability to attach a document to an email message for distribution greatly enhances the risk of copyright infringement. A user can be liable for the unauthorized copying and distribution of copyrighted material through email systems. Accordingly, employees should not knowingly copy and distribute through the email system any copyrighted material of a third party (such as software, database files, documentation, articles, graphics files and downloaded information) unless employees confirm in advance from appropriate sources that the City has the right to copy or distribute such material. Any questions concerning these rights should be directed to appropriate legal counsel.

*F. Email as a Record*

Generally, email messages are temporary communications that are non-vital and should be discarded routinely. However, depending on the content of the email, it may be considered a Public Record (see II. Definitions on page 2). Email generally should not to be used by City employees as a Public Record. However, in the event that any email meets the definition of a Public Record or contains information valuable for future reference for the employee or City, it should be saved outside of the email system by printing and saving the email as a paper document to protect and ensure retrievability over time. The rules of record retention apply regardless of the physical form or characteristics of the record. Even if an email is not a Public Record as defined in the Local Records Act, it is subject to the rules of discovery that govern litigation. Questions regarding record retention should be directed to the Office of Corporation Counsel.

*G. Deletion of Messages that are not Public Records*

The City strongly discourages the local storage of large numbers of email messages. Retention of messages fills up large amounts of storage space on the network server and can also slow down performance. In addition, because email messages can contain confidential information, it is desirable to limit the number, distribution and availability of such messages. If the message should be saved as a local record or Public Record, archive it within a week of receipt or generation. All other messages not subject to a litigation hold as instructed by the Office of Corporation Counsel should be deleted within two weeks of receipt or generation, if possible.

*H. Miscellaneous Considerations*

Email is a valuable form of communication which can help the City improve its quality of service. However, employees should consider the following matters when considering whether or not a message is appropriate for email communication:

1. Avoid making a statement in an email message about someone if you would not make the statement face-to-face with the person or write it in a formal memo.
2. Avoid making a statement in an email message which may be perceived as being ill-considered, uninformed, or offensive.
3. Avoid using email if a more time or cost effective communication is available (for instance, when a telephone conversation would be quicker.)
4. Avoid using email as a substitute for manager-subordinate face-to-face communications.
5. Avoid using email for personnel performance related communications.

*I. Employee Resignation*

All email correspondence is the property of the City. Employees who resign, retire, are laid off, or are terminated have no right to the contents of their email messages and are not allowed access to the email system. Supervisors with approval of the Director may access employees' email while

employees are on leave of absence, vacation, or are transferred from one department to another department if it is necessary for the City's business purposes.

*J. Email Signatures*

In order to project a more professional and consistent image with the public, City employees who use email should conform to the following signature policy:

Correspondence disseminated through the City's email system is considered official City business and property. It may also be considered public information depending on its content. Therefore, all electronic messages sent from City and utility email accounts will be uniform and consistent in the identification of the authors and/or senders.

Email signature blocks will be limited to the following: employee name and credentials (if any), job title, department address, telephone and facsimile numbers, email address and have the option to use the City's or utility's logo. Any information included in the email signature block that is not specified in this instruction will be construed as the inappropriate use of City email. Quotes, pictures, symbols, philosophical statements, or slogans are inappropriate in City email signature blocks.

A city department or organizational unit may request an exception to the standard email signature block for the purpose of communicating public information or the need for specific action to be taken by citizens. Requests for an exception must be submitted by the department head to the Director of Human Resources or designee in writing and will be reviewed and approved on a case by case basis.

The ban on the use of all quotes, pictures, symbols, philosophical statements, or slogans in the City email signature block is content neutral, not limited to any particular expression, and consistent with the City's obligations under constitutional law principles. As use of the City email system is intended for official City business, the use of quotes, pictures, symbols, philosophical statements or slogans may give the incorrect, and in some instances impermissible impression that the City officially endorses such quotes, pictures, symbols, philosophical statements, or slogans.

## *VI. Facsimile Machine Regulations*

*A. General Policy*

It is the policy of the City that facsimile machines (fax), like other City assets, are to be used for the benefit of the City. Use of fax machines to violate other City policies is prohibited and may lead to disciplinary action, up to and including discharge.

*B. No Expectation of Privacy*

Faxed documents may be read by others for a variety of valid reasons. Although this statement is also true of many other types of City correspondence, because of the nature of faxed messages they cannot be considered to be the private property of the sender or recipient. Transmittal of confidential information via facsimile is subject to the General Policy above relating to confidential information and is strongly discouraged.

*C. Prohibited Use*

In addition to the Unacceptable Uses outlined in the General Policy above, the following actions are prohibited:

1. Intercepting, or altering another person's faxed message.
2. Adopting the identity of another person on any faxed message, attempting to send faxed messages anonymously.
3. Misrepresenting your affiliation on any faxed message.
4. Composing and sending fax messages which contain racial or sexual slurs or jokes, or patently harassing, intimidating, abusive or offensive material to or about others.
5. Using a fax machine for any commercial promotional purpose, including personal messages offering to buy or sell goods or services.
6. Using fax machines to conduct employee organization, association or union business except that Union stewards and/or officers may utilize fax machines for the purpose of investigating or processing grievances. Such transmission will be primarily to expedite communication regarding such matters and will be reasonable with respect to time and volume.

*D. Confidential Information*

Employees are directed to the General Policy relating to confidential information for uses of all Information Technology Resources, including fax machines, set forth above. Use of fax machines to transmit confidential information is strongly discouraged. Confidential information should only be sent by fax machine when absolutely necessary to conduct City business. Examples of confidential information are set forth in the General Policy above. If you are unsure whether information is confidential, consult the Office of Corporation Counsel.

,

All faxed messages must contain a confidentiality legend in all capital letters at the top of the message in a form similar to the following:

"THIS MESSAGE MAY CONTAIN CONFIDENTIAL INFORMATION OF THE CITY OF SPRINGFIELD. UNAUTHORIZED USE OR DISCLOSURE IS PROHIBITED."

*E. Miscellaneous Considerations*

Fax machines are a valuable form of communication which can help the City improve its quality of service. However, employees should consider the following matters when considering whether or not a message is appropriate for faxing:

1. Avoid making a statement in a faxed message about someone if you would not make the statement face-to-face with the person or write it in a formal memo.
2. Avoid making a statement in a faxed message which may be perceived as being ill-considered, uninformed, or offensive.
3. Avoid using a fax machine if a more time or cost-effective communication is available (for instance, when a telephone conversation would be quicker.)
4. Avoid using a fax machine as a substitute for manager-subordinate face-to-face communications.
5. Avoid using a faxed message for personnel performance related communications.

## *VII. Internet Use Guidelines*

*A. Authorized Uses*

Directors, supervisors, or managers may authorize Internet use for communications and information exchanges relating to official City business.

*B. Use of the Internet*

Employees are directed to the General Policy set forth above which applies in all respects to use of the Internet. Use of the Internet is for City business only, with allowance made for reasonable personal use that does not otherwise violate this policy. Personal use will be considered reasonable if it meets the following criteria: (1) it does not adversely affect the employee's performance or official duties, (2) it is of minimal duration and frequency, (3) it does not violate any other employment policy or rule, or any federal, state or local law or regulation. Violations of this policy can result in disciplinary action up to and including discharge.

The Internet provides a source of information that can benefit many facets of City government. Electronic searches and retrieval tools allow users to gather information and data from a multitude of sources. Although this source of information can be very beneficial, it can also cause harm to an employee's computer, or even the City's Network through Spyware, viruses, worms, or other encroachments. Accessing web sites more specific to government and research organizations are considered more dependable and will diminish these types of intrusions for those who are authorized to access to the Internet.

Downloading software from Internet sites is strongly discouraged due to potential exposure to Spyware, viruses, worms, etc. Software should only be acquired over the Internet from reputable sources. Employees are encouraged to contact ISD if there is any doubt about a source.

No City correspondence or attached files should be transmitted through personal email accounts such as hotmail.com or yahoo.com. Only City-assigned email accounts should be used for this purpose.

*C. No Expectation of Privacy*

The City reserves the right to monitor and/or log all Internet activity with or without notice, including email and all web site communications, and therefore, employees should have no expectation of privacy in the use of these resources.

*D. Prohibited Uses*

In addition to the Unacceptable Uses outlined in the General Policy above, it is unacceptable for an employee to use, submit, publish, display or transmit on the Internet or on any computer system any information which:

1. Violates or infringes on the rights of any other person, including the right to privacy
2. Contains racial or sexual slurs or jokes, or is patently harassing, intimidating, abusive, or offensive to or about others
3. Restricts or inhibits other users from using the internet or the efficiency of the computer systems
4. Uses the Internet for any illegal purpose
5. Uses the Internet for commercial promotional purposes, including offers to buy or sell goods or services.

*E. Electronic Mail (Email)*

Internet email is subject to the Email Policy Guidelines set forth above.

*F. Passwords*

Access to the Internet the City's Network requires a password, and employees are prohibited from giving their passwords to any other person. The password remains the property of the City.

Employees are responsible for the confidentiality of passwords assigned to them. Divulging passwords may lead to disciplinary action.

## *VIII. City Telephone Use Policy*

### *A. Authorized Use*

The use of City telephone equipment and services is limited to official City business. However, official City business calls include emergency calls and calls that are in the best interest of the City. A call shall be considered as authorized and in the best interest of the City if it meets the following criteria:

1. It does not adversely affect the performance of City business by the employee or the employee's department.
2. It is of reasonable duration and frequency.
3. It could not have been reasonably made during non-work hours.

### *B. Personal Long Distance Calls*

A personal long distance call made during working hours is permitted if:

1. It is charged to the employee's home phone number or other non-government number;
2. It is made to an 800 toll-free number;
3. It is charged to the called party if a non-City number; or
4. It is charged to a personal credit card.

For any use of City telephones beyond the parameters of this policy an employee shall be charged actual City billed charges.

### *C. Reimbursement*

The employee shall reimburse the City for personal long distance calls by personal check payable to the appropriate fund. If the department presents a statement of itemized telephone calls to a City employee and the employee fails to reimburse the City voluntarily within 30 days for those calls which fall outside the parameters of the telephone usage policy, the employee shall be charged actual City billed charges plus $1 per minute for long distance calls. These rates are intended to cover the cost of the calls and the administrative costs associated with reviewing bills and processing payments. If not paid within 30 days of billing, collection action will be instituted through appropriate legal means.

An employee is put on notice that the payment of toll and other charges does not prevent the agency from instituting appropriate disciplinary action.

### *D. Use of Speakerphone*

Employees are reminded of the General Policy relating to confidential information. Use of a speakerphone/handsfree feature increases the likelihood of improper disclosure of confidential information. In many circumstances, use of speakerphones is also disruptive of a quiet work environment. For these reasons, speakerphone use should be minimized unless required when multiple persons in the same room are parties to the telephone conversation. Speakerphones should only be used in an enclosed area with all doors closed and the conversation must be incapable of being heard by persons not a party to the conversation. In all cases where more than one person is capable of listening to a telephone conversation via speakerphone because the additional person or persons are located in the enclosed area where the speakerphone is being used, the party or parties on the other end of the telephone conversation must be immediately

notified that such additional persons are in the enclosed area and are capable of listening to the telephone conversation.

## *IX. Photocopying Policy*

### *A. General Policy*

All photocopy machines and their supplies are the property of the City and are for City use only. City copiers have the capability to scan and disseminate documents to email accounts. As with other forms of communications, great care should be taken to assure the confidentiality of information.

An employee who uses copy machines and/or supplies for personal use is subject to discipline up to and including discharge as well as the assessment of monetary charges. An employee may be charged $.15 per copy for personal copies.

## *X. Other Policies Relating to Information Technology Resources*

### *A. Administration*

The domain names for the City's Internet sites are cwlp.com, Springfield.il.us, and LincolnLibrary.info. Assignment of email addresses will be the responsibility of the Information Systems Division. The standard naming convention will include the user's first name and last name separated by a period (i.e. John.Doe@cwlp.com). ISD shall be responsible for the day-to-day design, configuration, operation and maintenance of the City's email system.

### *B. Wireless Communications*

This policy covers all devices (e.g., personal computers, laptops, email-enabled cellular phones, PDA's, etc.) that connect to the City Network through a wireless communication mechanism. This includes any form of device capable of receiving and transmitting packet data over a wireless network. Prior to accessing the City Network through any wireless communication mechanism, an employee, contractor, vendor, volunteer, or third-party entity must complete a Network Security Request form, have it signed by the director or his/her designee, and submit it to ISD for approval. Approval of wireless connectivity to the City's Network will be granted only if the wireless communications mechanism:

- Is City-owned.
- Is reviewed, approved, secured, maintained and managed by ISD.
- Maintains point-to-point hardware encryption of at least 128 bits over the wireless link using WPA2 for encryption.
- Maintains a hardware address that can be registered and tracked.
- Support strong 802.1x authentication using an authentication server to be determined by ISD including but not limited to Cisco Secure ACS, Microsoft Internet Authentication Server, or another industry standard RADIUS server.
- Is password protected.
- Adheres to keeping the device in a secured location at all times.

Any waiver of this policy must be approved by the ISD Director and will be considered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request.

### *C. Remote Access*

Those wishing remote access to the City Network must complete a Security Request Form signed by the Director. Great care should be given to protecting the City's technical assets by always having

protective measures. Prior to allowing remote access, employees must adhere to the following guidelines:

- All remote computers must have ISD-provided or approved anti-virus software installed on the computer.
- Must have ISD-approved two-factor authentication hardware or software installed.
- Should utilize complex passwords as defined below:
- Password should not contain all or any part of the user's account name
- Should be at least six characters in length
- Contain characters from three of the following four categories:
    a. English uppercase characters (A through Z)
    b. English lowercase characters (a through z)
    c. Base 10 digits (0 through 9)
    d. Non-alphabetic characters (for example, !, $, #, %)
- Any files belonging to the City must be encrypted using encryption methodologies approved by ISD (please see Exhibit B. File Encryption Procedures).

*D. File Sharing*

No files with sensitive or confidential information can be provided to any third-party organization or individual without a completed Data Sharing Authorization Form (Attachment B) signed by the Director or ISD Director. These third-parties are not allowed to forward these data files to other entities without written permission of the Director. All data files remain the property of the City.

*E. Encryption of Messages and Other Data*

Encryption of any email message or other data file is prohibited unless specifically authorized to do so and without depositing the encryption key with the ISD's Security Administrator, Director or Director's designee prior to encrypting any messages or data files. If an employee is allowed to encrypt email or data files, this does not mean that the encrypted email or data file is intended for personal communication or use, nor does it suggest that this encrypted material is the private property of the employee.

*F. Hardware and Software Products*

The ISD shall have the responsibility for making hardware and general software recommendations for City departments. ISD is primarily responsible for maintaining most of the City's equipment and is trained in compatible, industry-standard hardware and software products. Please see Exhibit A. ISD Hardware Recommendations for the latest recommendations. Departments should be aware that Purchase Requisitions for computer equipment not previously approved by ISD will be delayed by Central Purchasing in order to seek the approval of ISD in conjunction with the normal purchasing approvals. Only City-owned software and hardware can be installed on City-owned equipment. All software must be licensed and must be used on the equipment for which it was purchased. All software licenses shall be recorded as: "City of Springfield, IL" or "City of Springfield, IL – Office of Public Utilities." The department name should be used on the license agreement instead of an individual's name. It is the policy of the City of Springfield that no employee use or install illegal software programs. Violations of software license agreements can result in liability to the City as well as the employees involved in the unauthorized use of proprietary software. Employees in violation of this policy will be subject to disciplinary action. At all times sufficient security measures and controls must be maintained with all equipment, software, and data, as well as maintaining the capability to backup and restore data.

*G. Computer Installation*

Departments wishing to have their computers or printers installed should complete a Request for Installation Form (Attachment C). Please complete one form for each piece of computer equipment that is to be installed by ISD. Please log on to the City's Intranet for more detailed information.

*H. Surplus Equipment*

The City Council approved an ordinance authorizing the ISD to determine and potentially declare computer-related equipment as surplus. The ordinance also authorizes ISD to transfer the surplus equipment to a third-party vendor for disposal in an environmentally safe manner. Departments wishing to dispose of equipment must complete a Surplus Computer Equipment Form – Individual Item (Attachment D). Or, if there are multiple items for disposal, use the Surplus Computer Equipment Form – Multiple Items (Attachment E) and forward to ISD. Please log on to the City's Intranet for more detailed information.

*I. Loaner Equipment*

A Loan Equipment Authorization Form (Attachment F) shall be completed prior to the use of any equipment on loan from the Information Systems Division.

*J. Surveillance Cameras*

In conjunction with the Department of Homeland Security and the Electric Transmission, Distribution and Operations Department, ISD has developed standards for purchasing web-enabled surveillance cameras and associated software licenses for City departments. These standards will provide for consistency across all departments enhancing a broad base of security that, in the event of an emergency, allows Homeland Security's Emergency Operations Center (EOC) personnel to utilize the cameras for monitoring if necessary. Please see Exhibit C. Network Camera Hardware for further information.

*K. USB Storage Devices*

To minimize potential virus and malware uploads, only authorized, city-issued USB storage devices are allowed. Employees who are required to use a USB storage device for their job must complete a Network Security Request Form signed by their director or manager prior to using the device (please see link in Attachment A or access ISD's online Network Security Request Form on the city's intranet).

Employees are responsible for the proper use of city-issued USB storage devices at all times. Lost or stolen devices must be reported by employees as soon as possible to their director or manager and to ISD by submitting an ISD Help Desk request. ISD will immediately de-authorize the device.

Employees may use authorized USB storage devices when collaborating with vendors, but the device must be de-authorized by ISD prior to leaving city property and no longer under the physical control of the employee. This can be done by submitting an ISD Help Desk request.

USB storage devices for use or provided by vendors or consultants must be pre-authorized prior to use on the city's network and will be registered by ISD to the employee responsible for the vendor or consultant (please see link in Attachment A or access ISD's online Network Security Request Form on the city's intranet).

Additional information regarding consultants and vendors and the use of City Information Technology Resources is provided in the IT Policy for the Use of Information Technology Resources Summary for Consultants and Vendors.

Any confidential files must be encrypted using encryption methodologies approved by ISD (please see Exhibit B. File Encryption Procedures).

*L. Mobile Devices*

Lower prices and the practicality of mobile devices such as Android tablets or Apple's iPads allows employees more flexibility to perform their job duties while away from the office. However, security remains a concern to the city's network due to malware or other mobile cyber security threats. As a result, ISD uses protective software to regulate usage such as, which business-related applications that can be downloaded or restricts websites that can be accessed, similar to the office environment.

Employees are responsible for the proper use of city-issued mobile devices at all times. Passwords must be used to restrict unauthorized access. Lost or stolen devices must be reported by employees as soon as possible to their director or manager and to ISD by submitting an ISD Help Desk request. ISD will immediately de-authorize the device.

When employees are issued a tablet or iPad, they must first upload the AirWatch security application. This will allow access to the city's network, mobile applications and emails. Should an employee require additional access beyond pre-defined mobile apps, they must submit a Security Request Form signed by their director or manager.

Vendors or consultants who use tablets must also install the mobile security application prior to being allowed access to the city's network. When no longer required, they will need to delete the application from their device.

Additional information regarding consultants and vendors and the use of City Information Technology Resources is provided in the IT Policy for the Use of Information Technology Resources Summary for Consultants and Vendors.

Any confidential files must be encrypted using encryption methodologies approved by ISD (please see Exhibit B. File Encryption Procedures).

## *XI. Assumption of Risk*

The City will make a good faith effort to keep the City Network system and its available information accurate. However, employees acknowledge that there is no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of any of the data or information available. For example, and without limitation, the City does not warrant that the City Network will be error free or free of computer viruses. In making use of these resources, employees agree to release the City from all claims of any kind, including claims for direct or indirect, incidental, or consequential damages of any nature, arising from any use or inability to use the City Network, and from any claim for negligence in connection with the operation of the City Network. Employees further acknowledge that the information available through interconnecting networks may be inaccurate. The City has no ability to maintain the accuracy of such information and has no authority over these materials. The City makes no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of the data and/or information residing on or passing through the City Network from outside networks. Use of the City Network is at the risk of the employee.

## *XII. Policy Not a Contract*

This policy does not constitute a contract; the City reserves the right to change the policy at any time.

## *XIII. Violations of this Policy*

Violations of this policy can result in disciplinary action up to and including discharge. All email messages are subject to all state and federal laws and rules which may apply to the use of email. Violations of certain provisions in this policy may subject an employee to possible civil and criminal liability under applicable federal and state laws. In addition, violations of this policy which are of a criminal nature may be referred for criminal prosecution.

## *XIV. Acknowledgment of Policy*

No person shall be granted access to Information Technology Resources until the person has acknowledged that he or she has read and fully understands this Policy for Use of Information Technology Resources and has agreed to adhere to and be bound by all provisions of the policy by signing a copy of the form attached hereto as Attachment G.