City of Baraboo
TECHNOLOGY USE POLICY

City of Baraboo - Information Technology Committee

This document serves as a reference guide to the policies of City of Baraboo Government regarding the use of City information technology resources

	Review Date	Revisions
Attorney Review	March 4, 2019	
Council Review and Approval	April 9, 2019	

S:\Administration\Information Technology\Tech Use Policy\Tech Use Policy - Final.docx

1) **INTRODUCTION.** In order to maximize the benefits of the information technology resources of City of Baraboo, the IT Committee has developed this Technology Use Policy to serve as a guide for City employees and elected officials who utilize the City's technology resources. The IT Committee's guiding principles are:
   a) To support City operations and facilitate the continuous improvement of business processes, through the provision of knowledge, tools and support services to the information technology users of the City.
   b) Provide quality services and solutions.
   c) Be professional and customer focused – to our citizens, City employees, and business partners.
   d) Maximize our information technology investment by leveraging our solutions and services to the fullest extent possible.
   e) Promote the standardization of technology solutions, whenever feasible.
   f) Revise business processes to achieve maximum benefit from available application packages.

2) **POLICY GOALS**.
   a) Provide the capability to improve the processes of City government, through the provision of secure and effective technology solutions to City departments, other agencies and the public.
   b) Ensure the availability and security of our networks and information.
   c) Enable the ease of obtaining and sharing of data.
   d) Achieve IT standardization, where feasible.
   e) Expedite the recovery of critical systems.
   f) Minimize the disruption to user access for system maintenance.
   g) Provide quality, professional services.

3) **UPDATES TO THIS POLICY**. The IT Committee will make minor updates to this policy as needed and will communicate updates to all Department Heads and IT contacts, as appropriate. Substantial policy changes require the approval of the Common Council by way of the Finance/Personnel Committee. The IT Committee will also provide access to this Policy on the City website.

4) **DEFINITIONS**. As used in this Policy, the following words and terms shall have the following meanings:
   a) **Attachments** – Files created in other applications (such as a word processor or spreadsheet) that are incorporated into an e-mail message.
   b) **Blog** – Publically accessible web forum that contains an online personal journal with reflections, comments, and opinions; which often solicits commentary from readers or provides hyperlinks to other online resources.
   c) **Blogging** – The act of updating or contributing to a blog.
   d) **City** – The City of Baraboo.
   e) **Designated network storage location** – A network folder, database, file share, inbox, mapped drive, cloud storage or other network storage provided for the purpose of storing electronic information on a secure computer network. Such locations are secured and regularly backed up to protect against data loss Local device storage is not a Designated Network Storage Location
   f) **E-mail** – An electronically transmitted message, along with any attachments and any information appended by the e-mail system.
   g) **E-mail system** – Computer hardware and software system that allows personal computer users to send, receive and store messages, documents and files with other individuals or groups of people over an internal network or the Internet.

h) **Encryption** – A means of coding messages so they appear to be random characters. Encryption has two benefits. First, it prevents disclosure of sensitive information to unauthorized third parties. Second, encryption allows for authentication of the information sent.
i) **Flash drive** – Removable storage media which plugs into a USB interface on a PC.
j) **Freeware** – Programming that is offered at no cost.
k) **Instant message** – An electronic form of instant communication whereby users communicate using text messages displayed on their computer monitors.
l) **Information system** – All computer hardware (computer, servers, printers, etc.) software and connecting devices interconnected for the purpose of storage, retrieval and sharing of electronic information.
m) **Internet** – The World Wide Web, which is a worldwide computer network.
n) **Internet browser** – An application which displays Web Pages and other information found on the Internet. Internet Explorer, Mozilla Firefox and Google Chrome are commonly used internet browsers.
o) **Internet Service Provider (ISP)** – And entity that provides internet access, typically for a fee.
p) **IT** – Information Technology.
q) **IT Committee** – Label referring to the employees of the City who serve on the Information Technology Committee. The Committee members are appointed by the City Administrator. The Committee may also include employees of the Sauk Co. MIS.
r) **Malware** – Malicious program or code intended to do damage to any part of the Information System
s) **MDM (Mobile Device Management)** – Software systems used to secure mobile devices and enforce policy through remotely managed device control.
t) **Mobile device** – Any device used to access City's information resources from outside of the City's secure facilities or via any network connection other than City's private, secure network facilities.
u) **Network file system** – A managed file system, on file servers for the storage of data, usually designated drive letter, typically H: or S:
v) **Personal device** or **personal mobile device** – Any device not owned or provided to the employee or contractor by City.
w) **Protected Information** - Any information that is considered private, confidential, proprietary or sensitive for which access or release is restricted by policy, rule, regulation or law.
x) **Public Resource** – Includes not only City equipment, hardware, software or tangible articles, but also the employee's time expended while on duty with the City.
y) **Removable Storage Media** – Any storage device that is portable and can be used to transfer information from one computer to another (flash drives, SD cards, USB disk drives, etc.).
z) **Risk** – Those factors that could affect confidentiality, availability, and integrity of City of Baraboo's key information assets and systems
aa) **Sauk Co. MIS** – Stands for Sauk County Management Information Systems Department.
bb) **Shared folder –** A network storage location shared by a group of users on the network. Typically designated by the drive letter "S."
cc) **Shareware** – Software that is distributed free on a "trial basis" with the understanding that the user may need to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date (e.g., after 30 days, the user can no longer get access to the program). Other shareware (sometimes called "liteware," which provides the same visual interface, icons and components of its full software counterpart) is offered with certain capabilities disabled as an enticement to buy the complete version of the program.

dd) **Social network** – Publically accessible website or application which allows individual to create profiles for the purpose of meeting and interacting with each other.
ee) **Social networking** – The practice of using social network applications.
ff) **Social media** – An application designed to facilitate social networking (synonymous with Social Network).
gg) **Standard applications** – Those applications provided by the IT Committee to all computer users within the City's information system.
hh) **System Access Form** or **System Access Authorization** – A form available through Seamless Docs that is available to department heads and their designees that must be used to request system access permissions be granted to a user or updated.
ii) **URL** – Uniform resource locator, commonly called an "internet address." It is the textual address of a particular website or internet resource.
jj) **Users** – Information system end users including City employees, system vendors, consultants and public users.
kk) **Virus** – A malicious computer program designed to execute and replicate itself without the computer user's knowledge typically by attaching itself to other programs.

5) **SYSTEM ACCESS, SECURITY AND USE**. Access to computer resources is provided to users for the purpose of advancing the governmental functions of the City. This access imposes certain responsibilities and obligations on all users. Users are subject to all applicable City policies as well as local, state and federal laws.
   a) City Property. All data, e-mail, e-mail attachments, documents and other electronic information within the City's information system are the property of City.
   b) Department Specific Policies. A Department Head may provide for a stricter policy of electronic communication and information systems use than is set forth in this Policy.
   c) Expectation of Privacy. THERE IS AND SHOULD BE NO EXPECTATION OF PRIVACY OR CONFIDENTIALITY WHEN USING THE CITY'S SYSTEMS. As provided for in this Policy and pursuant to any applicable local, state and federal laws, the City has the capability and the right to view data and e-mail at any time for City purposes or security. This Policy does not supersede any state or federal laws regarding privacy, confidentiality and appropriate use.
   d) Investigations. As a user of the City's technology resources, you agree to cooperate with any investigation regarding the use of your computer and your activities associated with technology resources.
   e) System Access and Permissions. Access to City systems is granted at the request of a Department Head or their designee. Department Heads or designees wishing to obtain access, or update system access permissions for an employee, must fill out a System Access Form. The Form should be submitted at least two weeks prior to the time at which the access will be required.
   f) System User Accounts. Users are granted access to the City's network resources through password protected individual user accounts. Revisions to user profiles or account permissions must be approved by the user's Department Head or designee and must be requested in advance, via a System Access Form.
   g) User Account Responsibilities. The following apply to all user accounts on any City system:
      1. Users are prohibited from using any account name other than those they are assigned or given authorization to use by their Department Head or designee.
      2. Department Heads or designees wishing to access a particular user account must request such access from the City Administrator.

3. Users are responsible for all inquiries, entries, and changes made to any of the City's information systems using their username and password.
4. Users must not:
    a) Leave usernames and passwords where someone else may see/find them.
    b) Use their username and password to log other individuals into the system (unless required for training purposes or addressing system issues and they watch them use the system).
    c) Use the username and password of others, or any information system logged in under another username and password.
    d) Store passwords electronically unless they are encrypted and password protected, nor written down unless they are locked and accessible only to the owner.

h) Password Requirements. When supported by the technology, the City's information system configures systems to enforce minimum password requirements based on the security requirements of the particular system. For all other systems, users are encouraged to utilize these minimum requirements:
    1. All passwords must be a minimum of eight characters alphanumeric.
    2. Users are required to change passwords at a minimum of once every 90 days.
    3. User passwords are not to be shared except for problem resolution or troubleshooting with their Department Head or Sauk County MIS staff.

i) Permissions and Privileges.
    1. The IT Committee will periodically review user permissions and remove permissions no longer in use or required by an individual user.
    2. Department Heads or their designees are responsible to advise the IT Committee and the City Administrator and Sauk County MIS of changes to an employee's job responsibilities that impact the individuals need for system privileges by completing a System Access Form.

j) System Security. It is the responsibility of every user of the City's information systems to ensure the confidentiality and integrity of the information owned or managed by City. Users must adhere of the following:
    1. All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of Protected Information at all times.
    2. Users are required to monitor workstations and take measures to prevent unauthorized access and theft.
    3. When approached by an individual that may be able to view Protected Information to which they are not authorized, users are to minimize the system display or otherwise secure it so that the individual is not able to view the Protected Information.

k) Workstations and Information Systems.
    1. Workstations and information systems are to be used for authorized business purposes, however users may utilize workstations for personal use if it does not interfere with the City's business needs and pursuant to the terms contained in this Policy and the Employee Handbook.
    2. The City maintains security software to block malicious web sites. In addition, users must avoid using sites that are not known to be safe and substantially related to their job responsibilities.
    3. Workstations are to be placed in secure areas away from public view and display screens are positioned to minimize unauthorized viewing and/or access, whenever feasible.
    4. Software programs and applications must be licensed. The IT Committee maintains licensing information for all City standard applications.

5. Users with access to download data are responsible for managing and protecting it from unauthorized access, disclosure, and theft.
6. Removing the City's workstations from the premises:
    a) Laptops, notebooks, and smart phones may be taken offsite by employees or contractors, when approved by the City Administrator, as needed to perform their assigned job responsibilities.
    b) Department Heads must maintain a list of individuals authorized to take equipment offsite.
7. Users Must Not:
    a) Allow any other individual to use any of the City's workstations or information systems that are not authorized by the City to utilize them.
    b) Download any software to a workstation without prior approval from their Department Head or designee or the IT Committee. The IT Committee may remove unapproved software without advance notice to the user.
    c) Download any Protected Information from the City's information systems to store or use it on any other system or device, other than the device authorized for their use by the IT Committee.
    d) Open any suspicious emails or suspicious website links in emails. If uncertain an email or website is suspicious, don't open it and notify your Department Head or designee.
    e) Connect any workstation to the City's network or utilize information systems or workstations not owned by City, unless the IT Committee evaluates and approves such use.
    f) Use tools or techniques to break/exploit or disable security measures.
    g) Change operating system configurations, upgrade existing operating systems, or install new operating systems on City equipment.
    h) Connect to unauthorized networks through the City's systems or devices.

l) Acceptable Use. Acceptable use is defined as that which is lawful, ethical, reflects honesty, and shows restraint in the consumption of shared resources. The primary purpose for using the City's technology resources is to perform the governmental functions of the City. This includes, but is not limited to:
    1. Communication with, and providing service to, members of the public.
    2. Conducting the business of the City department or unit.
    3. Communicating with other employees for work-related purposes.
    4. Gathering information relevant to job duties or to expand expertise.
    5. Content created should be accurate. Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer has the potential to be reviewed by others. User data and documents are considered City assets and should be treated as such. For the purpose of protecting these assets, users should store all data files on the network file systems provided, as these files are backed up daily.

m) Prohibited Use. Employees are prohibited from engaging in the following activities, with the exception of those activities required in the fulfillment of an individual's job responsibilities for which they have received prior approval by their Department Head or designee and the IT Committee, as applicable:
    1. Monopolizing systems.
    2. Overloading networks with excessive data.
    3. Wasting computer time, connection time, disk space or other resources.

4. Use which exceeds “Limited Personal Use,” as set forth in Section 5(l) of this policy.
5. Use technology resources for personal gain, political purposes, or to support or advocate for non-City related business.
6. Create, distribute, upload or download any disruptive, abusive, harassing, threatening, or offensive messages including offensive comments or graphics about sex, race, gender, color, disabilities, age, sexual orientation, pornography, religious beliefs, political beliefs, or national origin.
7. Use technology resources for illegal or unlawful purposes or to support or assist such purposes.
8. Use technology resources for wagering, betting or selling chances or to support or assist such purposes.
9. Use technology resources for personal long distance telephone calls.
10. Attempt to circumvent or subvert system or network security measures, provide internal network access to any unauthorized users or use your account to gain unauthorized access to other networks and systems.
11. Mount an attack on the security of any system or attempt to hack or introduce viruses into any system.
12. Use the network in a manner that may disrupt network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses or malware, and sustained high volume network traffic.
13. Intercept network traffic for any purpose unless engaged in authorized network administrative duties.
14. Install encryption software on any City computers without first obtaining written permission from your department head and the IT Committee. Users may not use encryption keys or encryption technology that is unknown to their department head or the IT Committee.
15. Engage in online fundraising.
16. Engage in mass-mailing, “everyone e-mails,” or send City-wide messages without department head, the IT Committee or City Administrator approval, as applicable.
17. Send or forward mailings about viruses or other warnings about outside computer attacks to users other than their Department Head or designee or the IT Committee (these are almost always a hoax and should not be propagated).
18. Initiate or forward chain letters by e-mail.
19. Spoof (disguise) your identity or send anonymous e-mail or send e-mail under another employee’s name.
20. Forge header information or any use that does not appropriately and accurately identify the sender.
21. Download any non-standard or non-business related files or software, including "freeware" and/or "shareware" programs unless previously approved by the IT Committee.
22. Load personal ISP email accounts on City owned equipment.
23. Disburse or share any City data not authorized by their department head or designee and relevant to the job being performed, or any data considered protected, unless expressly authorized to do so in the performance of one’s job responsibilities.
24. Make or use illegal copies of copyrighted software or other mediums, store such copies on City systems, or transmit them over the City network.
25. Any activity not deemed to be in the best interest of the City.

26. Any activity that compromises the security or integrity of the City's information system.
27. Any activity that violates any City ordinance, including the City of Baraboo Code of Ethics, Federal, State or local laws.

n) Informing Employees. It is the responsibility of the Department Head or designee to be aware of how the City's information system is being utilized by his/her employees and ensure that employees are periodically informed and aware of the IT Committee policies. If a Department Head or designee suspects any employee is violating this Policy, they should contact the City Administrator.

o) Limited Personal Use.
   1. Authorized users may use the internet and e-mail for limited personal use. This is defined as any personally initiated computer based activity (email, internet browsing, etc.).
   2. Limited personal use is a privilege, not a right, and may be limited or removed at any time and is subject to the terms and conditions of this Policy.
   3. The City does not accept liability for any loss or damage suffered by an employee as a result of using the City internet connection for personal use.
   4. Improper personal use of the City's information systems could result in disciplinary action.
   5. Occasional, limited, appropriate personal use of the computer system is permitted, provided such use does not:
      a) Interfere with the user's work performance.
      b) Interfere with the normal operation of your department or work unit.
      c) Interfere with any other user's work performance or have a negative impact on overall employee productivity.
      d) Have an undue impact on the operation of City systems.
      e) Have a negative impact on the public's perception of work duties.
      f) Cause any additional expense or load to the City or department.
      g) Compromise a department or the City in any way.
      h) Engage in concerted work activities of any kind.
      i) Violate any other provision of this policy, or any other policy, guideline, law, regulation, or standard.
      j) Violate departmental policies or standards of an employee's department. In limiting personal use, the City expects employees to exercise the same good judgment that they would use in all work situations regarding personal activities.

p) System Monitoring. All computer applications, programs, data and information, created or stored on City information systems is the property of City. The City may monitor this information without prior notice. The City reserves the right to access any information stored, created or received on the City's information systems. The reservation of this right is to ensure that public resources are not being wasted, the City's business is carried out and to ensure the City's information systems are operating as efficiently as possible. Monitoring or access may be exercised under any of the following circumstances:
   1. Performance testing or problem solving purposes.
   2. As necessary in the course of an investigation for possible violation of City policies.
   3. If there is reasonable suspicion that a user has committed, or is committing a crime against the City or for which the City could be liable.
   4. Random or automated monitoring to ensure that content is in compliance with the business's established policies.
   5. A request for monitoring made by appropriate authority.
   6. When required to do so by law.
   7. To perform a task or project in an employee's absence.

6) **ELECTRONIC COMMUNICATION: E-MAIL**. Electronic communications provide a fast and efficient method of communicating. The City's information system provides such capabilities for the purpose of conducting City business. Upon Department Head or designee's request, the City will authorize an e-mail account, which includes an internet e-mail address, to users. In addition, a Department Head or designee may require an instant messaging account for employees with an authorized email account on the City's email system.
   a) Account Creation and Administration.
      1. E-mail account creations or removals must be requested by a Department Head or designee two weeks in advance with a System Access Form.
      2. Changes to e-mail accounts require two weeks notification and Department Head or City Administrator approval.
      3. With the City Administrator's approval, user accounts will be deleted after the termination of employment. However, an employee may request their user account be maintained and e-mail forwarded for up to 60 days, subject to the City Administrator's sole discretion, after which the user account will be deleted.
   b) Limited Personal Use. While it is the intention of the IT Committee that the e-mail system be used for City business, limited personal use, as defined in Section 5(l), above, is permitted, provided such usage is deemed appropriate by the individual's supervisor and does not impede any individual's ability to perform their job or violate any of the other provisions of this policy.
   c) Account Use and Security.
      1. Inappropriate use of the e-mail system may result in disciplinary action up to and including termination.
      2. E-mail accounts may be used only by the intended user. Use by anyone other than the named account's owner is not permitted except as provided by subsection (e), below.
      3. It is the account owner's responsibility to maintain proper password protection and take reasonable precautions to prevent unauthorized use when the employee is absent for an unanticipated or extended period of time.
      4. Users are cautioned to remember that unencrypted, unsecured email may be intercepted, forwarded and altered.
      5. City e-mail addresses are not to be used as contact addresses for solicitations, account bids, chat rooms, social networking, blogs, subscriptions, etc., not related to City business.
   d) E-mail Records Retention.
      1. E-mail and attached documents are the property of the City.
      2. Many e-mail messages represent temporary communications that are non-vital and may be discarded routinely. However, depending on the content of the e-mail message, it may be subject to the City's records retention policies and ordinances. E-mail falling under this category must be retained as required pursuant to City's information practices ordinance and shall only be destroyed in accordance with that authority. **E-mail users must adhere to the City's records retention ordinance.** Refer to Section 1.60 of the City of Baraboo Code of Ordinances for more information.
      3. Email messages may be automatically archived and users are cautioned to be aware that deleting an e-mail message from a mailbox does not delete all copies of the message. The City reserves the right to establish policy that e-mail messages will be retained on the City's e-mail server for finite period of time and then deleted.
   e) Monitoring & Access.
      1. It is not the practice of the City to routinely monitor email activity or content. As necessary, Department Heads or designees, the City Attorney, the City Administrator, IT

staff (including Sauk Co. MIS) and consultants, and law enforcement may access e-mail accounts for business purposes. Such purposes may include but are not limited to:

a) System maintenance.
b) Troubleshooting.
c) Performance monitoring.
d) In order to fulfill records request.
e) In the course of a legal or internal investigation.

2. Employee's e-mail accounts may not be monitored for disciplinary purposes without first contacting the City Administrator and City Attorney.
3. To ensure the continuity of operations, managers and supervisors may, with department head approval, request access to an employee's e-mail if the employee is on leave of absence, extended leave or terminated.

f) Off-Site Account Access (Web Mail).

1. All email accounts are setup to allow the user off-site access through a web browser.
2. Passwords are synced with the City's network.
3. Off-site access is for use only while performing work-related tasks.
4. Access may be terminated during periods of extended leave.
5. Off-site access to an e-mail account does not constitute approval for compensation for work performed from outside of City premises. For non-exempt employees, prior approval from your department head is required for compensation.

7) **INTERNET USE.**

a) Internet Accessibility. The internet is a powerful tool for research, procurement, and communication. The City will provide internet connectivity to users who require it to effectively perform their duties for City. Internet accessibility for individuals may be requested by a Department Head or designee via a System Access Form and should be requested two weeks in advance.

1. Only the individual(s) assigned or authorized to a computer workstation may access the internet from that station. Use by other individuals to access the internet constitutes a violation of this policy, unless approved by the individual's department head or designee.
2. Individuals who have been granted internet access are responsible for appropriate use. It is the intention of the City that internet access is provided for the purpose of performing City business, although limited personal use, as discussed in Section 5(l), above, will be allowed.
3. All internet activity on the City's network is logged by URL. The City may use this information in the assessment of system performance, troubleshooting and monitoring of appropriate use.
4. The City reserves the right to block access to any internet site deemed to be malicious or in conflict with any City policy.
5. Inappropriate use of the internet, as defined in Section 5, above, may result in loss of internet access and disciplinary action up to and including termination.

b) Safety and Security. Use of the internet incurs certain risks and it is up to the user to exhibit caution and good judgment when accessing internet content. Some internet websites are infected with viruses and malware, which may be downloaded to the user's workstation without any interaction from the user. The following guidelines should be adhered to when browsing from City computers:

1. Avoid unknown websites.
2. Do not install or activate any unexpected installations or downloads.

3. Do not respond to messages or click on links from unknown sources
4. Contact your Department Head and/or the Sauk Co. MIS Helpdesk (see Section 11, below) immediately if you encounter an unexpected or suspicious download or virus warning.

c) Objectionable Content. A wide variety of information is available on the internet. Some individuals may find this information offensive or otherwise objectionable. Users should be aware that although the City may utilize filtering to avoid objectionable material, it does not have complete control over the Internet and can therefore not be responsible for the content of information available.

d) Blogging. The use of blogs on City computers is discouraged unless such use is necessary in the performance of an individual's job responsibilities. Blogging activities on City computers are subject to all provisions of this Policy and all other policies of the City.

e) Instant Messaging and Chat Rooms. Users may only engage in chat rooms, instant messenger communications or newsgroups if it is required as a part of their job requirements and has been approved by their Department Head or designee. Questions about these services should be referred to the IT Committee.

f) Social Networking and Social Media. Unless specifically required in the performance of an individual's work activities, social networking and the use of social network sites is prohibited on City systems. These sites often present security risks due to malware and computer viruses If an employee does access social network sites for authorized purposes, in addition to the terms and conditions set forth elsewhere in this policy, they are subject to the terms and conditions found in the City of Baraboo Social Media Use Policy.

g) Use of Fee Sites. Users who access any internet sites for which a charge or a fee is involved, without the written consent of their Department Head or designee, may be held responsible for any and all payments associated with visiting that site.

h) Use during Non-Work Hours. Access to the internet during a user's non-work hours via City equipment requires adhere to all provisions of this Policy and cannot conflict with the best interests of the City.

i) High Bandwidth Applications. Accessing entertainment, games and other websites that use significant bandwidth could jeopardize network speed for other business uses and should be avoided. This includes websites that broadcast radio, TV, video, or any streaming technology, and other similar high-bandwidth sites that are not related to City business.

j) Suspension of Internet Access Privileges. User internet access is at the discretion of a Department Head or designee and may be suspended at any time. Use may also be suspended in the event of a continued breach of this or any other policies through the internet usage of a specific user. In addition to the suspension of internet access, improper use may result in disciplinary action up to and including termination.

8) **NETWORK COMPUTER USE.** The City's information network provides connectivity for City departments to centrally managed systems. These systems provide communications, data security, storage and external connectivity via the internet.

a) Network Storage. Network user accounts provide access to designated network storage locations. Each individual account is assigned a "Home" network folder, designated by the drive letter H:, which is not shared with other users; and a "Shared" network folder, designated by the drive letter S:, which is shared with other users within the department or business unit. In addition, other storages locations (drives) may be designated for application specific storage.

b) Data Backup. The City will provide regular backups of all data stored to the City's designated network storage locations. These backups provide the capability to restore a system or file share in the event of loss due to device malfunction, file corruption or catastrophic system failure. To

ensure the successful backup of all critical data files must be closed and available to the backup system.

1. All users should close all files and log off at the end of the day.
2. Files should only be stored to designated network storage locations and not be stored on the desktop workstations local storage devices.
3. Data stored on laptops for mobile use should be synchronized to system or network storage regularly.
4. Requests for the restoration of accidentally deleted or corrupted files from backup should be made to the Sauk Co. MIS Helpdesk (see Section 11, below).
5. Deleted files are temporarily retained in the backup system, as determined by the IT Committee.
6. Backup copies do not provide permanent retention and are not suitable for proper records retention.

c) Attachment of Equipment or Other Devices. Prior approval from your department head must be obtained before any equipment is attached to the City network or to a City computer (these provisions do not apply to the City's public Wi-Fi network). When using the City's private network resources, users may not:

1. Connect any networking devices to the City network.
2. Make connection to individual servers / desktops / workstations for remote access purposes, without prior approval from the user's supervisor and the IT Committee.
3. Allow non-City agencies or entities to access the City network without prior IT Committee approval.

d) Removable Storage Media. The use of removable storage media presents a risk for the loss of data or the accidental release of confidential or private information. Removable storage devices also provide a vehicle through which computer viruses may be spread. Users who have a need to use these devices are cautioned to do so in a manner that reduces these risks and adheres to the following guidelines:

1. Use must be approved by the user's Department Head and the IT Committee.
2. It is recommended that the device be obtained through your Department Head.
3. Only non-confidential or public information may be stored on such devices, unless the device is encrypted, password protected and the user has obtained authorization from their department head or designee and the IT Committee.
4. User accepts the responsibility of protecting any information stored on the device.
5. Devices used to store City information should not be used for any other purpose.
6. Lost devices should be immediately reported to the user's Department Head and the IT Committee.

e) Unauthorized Software. Use of unauthorized software may degrade the performance of the City's systems, create security risks, reduce employee productivity and expose the City to copyright liability.

1. Users are prohibited from installing applications, plugins, etc., on their City workstation without receiving approval from the IT Committee prior to installation.
2. Software installations not approved prior to the instillation by the IT Committee may be considered unauthorized and will be subject to removal.
3. The IT Committee will immediately remove any unauthorized software in use, when encountered, unless the software has a legitimate business purpose for the user, is appropriately licensed and approved by the user's supervisor. The IT Committee will work with the Department Head to address any legitimate business need before removal.

4. It is the responsibility of all users to comply with maintaining City standards and protecting computing resources by not downloading or installing unauthorized software.
5. According to the US Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $150,000 per work copied, and criminal penalties, including fines and imprisonment. Users who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination. The City does not condone the illegal duplication of any copyright protected material.

9) **MOBILE DEVICES**

a) Use During Working Hours. The use of mobile devices in the workplace can be distracting and disruptive. Employees using approved mobile devices in the work place are required to do so in a manner that is respectful and non-disruptive.
   1. The City discourages the non-work related use of personal mobile devices during working hours.
   2. Employees are asked keep personal devices off or silenced and limit their use to breaks, outside of common work areas, and are to avoid inappropriate discussions and interrupting or distracting others
   3. Each department may have its own policy related to these devices. Employees should consult their Department Head, manager or supervisor for additional guidance.

b) Approved Use.
   1. Employees wishing to have mobile access to the City's information systems must have a legitimate business need for such access and obtain approval from their manger or supervisor. Mobile access to the City's information systems must also be reviewed and approved by the City Administrator and a Mobile Device Authorization Request Form is to be submitted to the IT Committee describing the work related need and the information to be accessed.
   2. Approval and work related use of an authorized mobile device is subject to the terms and conditions set forth in the City of Baraboo Employee Policy and Procedure Handbook as well as in this Policy.
   3. Generally, access to City information will require a City issued device. However, under some circumstances, when information to be accessed is not considered to be Protected Information, a personal mobile device may be configured for system access. This is provided that such device may be configured to meet all requirements for mobile access set forth by City policies, subject to review and approval by the IT Committee. Any and all mobile access to the City's information resources is subject to these terms and any other related City policies.

c) Appropriate Use of City Owned Devices. Mobile devices used to conduct the business of the City are subject to same appropriate use guidelines as any other computing device. Additionally, the following shall apply to mobile devices owned by City of Baraboo:
   1. The City Administrator may authorize employees to use a City owned mobile device as a personal mobile device, in addition to a business device, contingent upon the employee signing a waiver and release and agreeing to reimburse the City for the employee's personal use of the mobile device. The waiver and release must be signed by both the employee and the City Administrator prior to the issuance of a cell phone and will be kept in the employee's personnel file.
   2. Employees provided a City owned mobile device but not authorized to use said device for personal use may not use the device for personal use unless all of the following are met:

a) No additional costs are incurred by the City or, if incurred, the employee promptly reimburses the City for said costs.
b) The use is for emergency purposes or is authorized by manager or supervisor.
c) The use does not violate the terms set forth in this and other related City policies.

3. City owned devices must be properly secured at all times to prevent loss, theft and unauthorized access.
4. The loss or damage of a City owned device may lead to disciplinary action and may also result in the employee being required to reimburse the City for the cost of the device. The decision to take disciplinary action and/or to require reimbursement will be decided on a fact-specific basis as determined by the City Administrator or designee.
5. Mobile devices should not be used while driving or operating equipment unless they have a "hands free" capability and are being used hands free.

d) Work Related Use of Employee Owned Devices.

1. The use of personal mobile devices approved under this section is subject to the same terms and conditions as a City owned device when being used for work related purposes.
2. The use of a personal device for City business may subject the device to Wisconsin's open records laws. Any information stored on the device is subject to review by the City or other government entities.
3. The use of a personal device for work related activities is permitted only at the request of the device owner and upon approval by the Department Head or designee. When such use is requested by the device owner, the Department Head must evaluate whether the employee's use of their personal mobile device for work purposes is routine or essential to the employee's job performance or if it will be occasional and non-essential. If the use is more than occasional and/or is essential to the performance of the employee's job, the Department Head should consult with the City Administrator about having the employee be issued a City owned device.
4. Any risks associated with such use are the owner's sole responsibility. The City will not be responsible for:
    a) Damage or malfunction caused by the configuration of the device for work related activities.
    b) Provider service charges for work related activities.
    c) Costs incurred by loss or theft of the device.
    d) The loss of any information stored on the device.
    e) The support or repair of the device.
    f) Compensation for time spent accessing City information on the device outside of an employee's regular work hours unless approved prior by the employees supervisor.

e) Loss or Theft of a Device.

1. Loss of any device used to access the City's information resources must be reported immediately to the Sauk Co. MIS Helpdesk (see Section 11, below).
2. Upon notification of the loss of a device, the IT Committee or designee will:
    a) Remotely lock out access to the device.
    b) Attempt to determine the location of the device.
    c) Work with device owner to locate the device.
    d) Issue the command to remotely wipe the device if it cannot be located.
3. Services to lost personal mobile devices, used for work related purposes, are not to be discontinued until the above activities have been completed and the City has authorized such service discontinuation.

f) Security. Mobile devices, authorized by the IT Committee for access to the City's information resources, are secured based on the classification of the information to be accessed by the device. The user is expected to comply with all policies related to the security of the City's Protected Information regardless of where or how such information is accessed. It is the user's responsibility to:
   1. Maintain appropriate passwords.
   2. Protect the device from loss or unauthorized access.
   3. Utilize all provided security safeguards.
   4. Notify the IT Committee of any suspected virus or malfunction.
   5. Ensure devices used to access Protected Information have the proper encryption.
   6. Transmit Protected Information via VPN connection.
   7. Avoid any use which may compromise device security.
   8. Refrain from disabling or circumventing installed MDM clients or security measures.

10) **RECORD RETENTION.** The City's Code of Ordinances, Section 1.60, Information Practices, formally adopts the State of Wisconsin Public Records Board's General Schedules for City Governments. Elected Officials, Department Heads and managers are responsible to ensure that records subject to this retention schedule are appropriately retained. Records may be retained in hardcopy or electronic format. For the purpose of this policy, records are presumed to be in electronic format. The following guidelines relate to the retention of electronic records created on City of Baraboo's systems. Refer to §1.60 of the City of Baraboo Code of Ordinances for specific information regarding retention of all City records.
   a) Records Custodian. Each department is responsible for the records created during its regular course of business. Unless otherwise prescribed by policy, ordinance or law, the department head is presumed to be the records custodian for a given department.
   b) Retention. Retention is the responsibility of the custodian of the record. To retain a record in an electronic format means to store such record to a designated network storage location. Do not store electronic records to a local workstation hard drive or removable storage location as such storage is subject to loss due to device failure, malfunction or theft.
   c) System Backups and Archives. System backups and archives are utilized to protect information from accidental loss due to system failure, disaster or accidental deletion. Backups and archives are not intended to be used for records retention. Files deleted from a designated network storage location will also be deleted from backups within a number of days. Likewise, information archives are periodically purged. To ensure the retention of the record in accordance with the prescribe schedule, a records custodian must save a copy in a designated network storage location.
   d) Email Archive. The City maintains a dedicated email storage archive to better facilitate records discovery for email record requests. Archives are not configured to fulfill specific records retention requirements and custodians are advised to retain copies of any and all records subject to retention in a designated network storage location.
   e) Records Requests. Records requests are to be directed to the custodian of the records requested. The IT Committee will assist custodians in locating records by utilizing available tools to search for records using dates, keywords and metadata, however, it is the custodian's duty to fulfill the request. All records requests should be reviewed by the City Attorney before any records are released.

11) **COMPUTER SUPPORT / TECHNOLOGY REQUESTS.**

a) Helpdesk. The City contracts with Sauk Co. MIS to provide certain network and workstation maintenance and software services through the MIS Helpdesk. There may also be members of your department designated to perform tech services to equipment and personnel. Please consult your department head for advice before calling the Sauk Co. MIS Helpdesk.
   1. The Sauk Co. MIS Helpdesk's normal business hours are 7:30am-4:30pm, Monday through Friday, and can be reached at 608-355-3555.
   2. For those departments that require 24/7 support, cell phone and/or pager numbers will be provided.
   3. You may also enter any non-urgent requests via the Helpdesk e-mail account at Helpdesk@co.sauk.wi.us.

b) Remote Access. Sauk Co. MIS Helpdesk personnel utilize remote access to aid is computer support and maintenance. Prior to remotely accessing a user's computer, when feasible, Sauk Co. MIS Helpdesk staff will notify the user in advance.

c) Outside Technical Support. Prior to contacting outside technical support for assistance with dedicated departmental applications, users are encourage to contact the Sauk Co. MIS Helpdesk to verify the problem and ensure that the issues they are experiencing are not part of a known issue. Contacting the Sauk Co. MIS Helpdesk will:
   1. Ensure a timely response by the appropriate resource.
   2. Avoid redundancy in support response.
   3. Ensure documentation of issue for tracking and future reference.
   4. Avoid unnecessary cost to the City.

d) Purchase Requests. All proposed purchases of computer software, hardware, and peripherals are to be submitted to the City Administrator or his/her designee before purchase. The City Administrator or his/her designee will determine if the purchases need review by the IT Committee. Authorization for purchases will come from the City Administrator or his/her designee. Departments will budget for purchases as per the work plan approved in their respective Departmental budget.

12) **SYSTEM ACCESS AUTHORIZATION REQUESTS.**

a) System Access Requests. System access request should be submitted to a Department Head or the City Administrator as they are the only people authorized to submit formal request to the Sauk Co. MIS department for services. The form is available at the City of Baraboo SeamlessGov web site: https://baraboowi-internal.seamlessgov.com/ or the Sauk County MIS web site: http://scm.co.sauk.wi.us/Internet/Applications/main.nsf/misforms.xsp

b) System Access Authorization Request. To initiate, terminate or modify a User's accessibility to City systems must be approved by the City Administrator or other designated City Staff and submitted to Sauk County MIS on their form at: http://scm.co.sauk.wi.us/Internet/Applications/main.nsf/misforms.xsp

c) Other Requests. Other requests, such as a Project Request (to request hardware or software changes or system modifications) and Mobile Device Request (to request mobile access to the City's information resources) must be directed to your department head. Department Heads are granted access to the Sauk Co. MIS forms system and may authorize other staff to submit requests and security access changes for City information systems on their behalf.

13) **COMPUTER TRAINING.**

a) Applications Training. Due to the diversity of applications used throughout the City, it is difficult to have a single training solution to meet the needs of all City employees. For this reason, it is

left up to the individual departments to determine the training needs of their employees. The IT Committee will facilitate this process by providing information regarding the training resources available and working with the individual departments in arranging training. Additionally, the IT Committee will periodically make available in-house training on those applications that are considered to be standard applications. This training will be for basic to intermediate level users and focus primarily on new employees.

b) Security Training. The City provides regular system security training to all employees via a web based training system. These training sessions are mandatory for all employees that access the City's information systems and the systems are configured to provide user tracking to ensure compliance. Users who do not complete the training will be referred to their supervisor or department head for disciplinary action.

14) **WEBSITES AND SOCIAL MEDIA SITES**. Website and social media sites are important tools for the provision of information to the public in a timely and easily accessible manner. The City encourages the responsible use of these tools.

a) City Website. The official City website at www.cityofbaraboo.com provides a home page for each City department. This is to be every department's primary web presence and home page. Additional websites and authorized social media portals must link from this home page.

b) Department Website. All internet content related to a department on is to be included on the departmental home page.

1. The accuracy and timeliness of internet content is the responsibly of the department head.
2. The department head may delegate the activity of updating their departmental home page by contacting the City Administrator's Office.

c) City Social Media Sites. There will be no more than one official City social media site on each social media platform (e.g., one official City Facebook page, one official City YouTube site). Each official social media site shall be run by the City Administrator or his/her designee.

d) Department Social Media Site.

1. A Department Head may elect to create no more than one official department specific social media site per social media platform (e.g., one department specific Facebook page, one department specific YouTube site), but only if the department's information would not be better shared on the main City sites.
2. If a department makes social media site(s), the department must include a link to this site(s) from their department home page and the City's official social media directory on the City's official website, and the department head must notify the City Administrator and the IT Committee.
3. The department is responsible for maintaining their social media site(s), including making regular postings to the site(s), training the employees authorized to post on the site(s), and ensuring the site(s) are up-to-date.
4. All social media sites must, at minimum, contain a link prominently displayed that directs the user to the Website and Social Media Site Terms and Conditions for the City of Baraboo, which is available from the City Attorney.
5. Employees posting to a social media platform on behalf of the City or department must not post any material that is copyright protected or otherwise in violation of this policy or the Employee Handbook.
6. By creating a social media site, a department creates a limited public forum for purposes of First Amendment protections. This means that the department is not able to indiscriminately monitor comments without potentially violating a person's constitutional

rights. This does not mean the City has to allow all comments. The best way to address comments on a department's social media page is as follows: "The opinions and comments expressed on this social media site may not reflect the opinions and positions of the City government, its officers, or employees. If you have any questions concerning this social media site, please contact the City Administrator's Office."

15) **INTERNET USE – WEB LINKING**. The City's website is used to enhance and promote the City, to make people aware of available community services, and to provide information about the City's operations and activities. THE CITY'S WEBSITE IS NOT A PUBLIC FORUM FOR EXPRESSIVE ACTIVITY. Having a website allows the City to link to other web sites consistent with the above purpose. This is typically done in order to provide related information to someone coming to the City's website. The City exercises no editorial control over any of the information contained in these other organizations' websites. In addition, the City has no control over decisions made by these other organizations as to their website links. As a result, it is possible that someone starting with the City's website could eventually link to information that may not be related to the City, or that the viewer may find offensive, or that may negatively impact the City's website purpose. Such links may interfere with the purpose to which the City's website is dedicated. While this cannot be totally prevented, we can attempt to minimize the probability of it happening by developing some guidelines that can be used in determining whether the City should link to an organization's website. The City is not responsible for the content of any web site to which it provides a link. This policy applies to all departments that have or maintain a website, including the City's primary website.

a) Guidelines for Website Inclusion on the City's Website.
    1. Government websites.
    2. Tourism websites related to the greater Baraboo area.
    3. Websites that contain community information, e.g., civic, recreational, educational, and the like, for the greater Baraboo area.
    4. School websites.
    5. Library websites.
    6. Websites that contain regional cultural information.
    7. Benevolent and charitable organizational websites that provide or promote local community services. h. Websites for organizations that are funded by the City.
    8. Websites of non-profit professional organizations of which the City or its agencies are members.
    9. Websites that contain information related to the greater Baraboo area deemed to be of use to the City, its citizens, visitors, or businesses.
    10. Websites of a similar character to sites listed above that would likewise support the City's website purpose.

b) Guidelines for Website Exclusion.
    1. Websites containing information promoting any illegal activities.
    2. Websites for which the focus is to market a particular commercial service or product (See Acknowledgments below).
    3. Websites containing information that would violate any of the City, state or federal Affirmative Action policies, Equal Opportunity Ordinance, Ethics Ordinance, or that may be in violation of any other City ordinances, or state or federal laws.
    4. Websites unrelated to the City of Baraboo and the surrounding community.
    5. Websites for a specific political candidate or political party. Rather, the City may link to independent organizations such as the League of Women Voters.
    6. Websites containing material that is harmful to minors.

7. Websites that are not consistent with the purpose of the City's website.
8. Websites containing material that is obscene, profane, defamatory, libelous, or fraudulent.
9. Acknowledgments. From time to time, a for-profit commercial company may partner with the City on a particular project and/or they may contribute toward a project. An acknowledgment for that company's contribution can be made on the City's website including the company's logo along with the acknowledgment is also acceptable. In keeping with the above guidelines, no direct link should be made to the company's website.

c) Decision Making Authority. The decision to link to an organization's web site can be made by each individual department or department head or their designee. The City Administrator is available for consultation to assist in the decision. Organizations wishing to appeal the decision of an agency should be instructed to submit their appeal in writing to the City Administrator. The decision of the City Administrator shall be final. Any denial of a request to provide a link should be documented and forwarded to the City Administrator. After consultation with the City Attorney, links will be removed if found to be in violation. The City reserves the right to limit the number of websites to which it links in order to ensure the usefulness and effectiveness of the website for its intended purpose.

16) **POLICY INFRACTIONS**

a) City employees who violate this Policy may have their IT access removed and may be subject to disciplinary action up to and including termination. In addition, contractors or other third parties who violate this policy may have their contract revoked. Other legal remedies, including criminal prosecution, may also be pursued if warranted.

b) It is the policy of City to handle infractions as follows:
   1. Policy violations must be reported to the user's department head.
   2. The user's department head should approach the violator(s) directly with the findings, ensure the user is aware of the policy, and give them the opportunity to cease and desist; or, depending on the severity, follow disciplinary procedures consistent with the guidelines and policies of the City of Baraboo Employee Handbook.