City of WHITEWATER		Information Technologies Policies & Standards			
Owner:	IT Director	Approving Position:	Common Council	Pages:	7
Issue Date:	12/22/2011	Revision Date:		Review Date:	
Special Instructions:	Minor updates to policy to reflect changes in IT technology and procedures such as ticketing system.				

I. PURPOSE

The purpose of this policy is to set forth general guidelines for the efficient, ethical and appropriate use of and prohibit inappropriate use of Informational Technology (IT) resources. All IT resources are the property of the City of Whitewater. Employees should not have any expectations of privacy and understand that the City can and will monitor use of all IT resources including the use of the City's Wi-Fi (Wireless Local Area Network) on personal devices. The policy is meant to ensure that the use of IT resources among employees is consistent with City policies, all applicable laws and the individual user's job responsibilities. The policy is intended to confirm that all information composed, sent, or received is and shall remain City property, and it further enhances City-wide coordination and management of electronic communications and IT resources. This policy is intended to apply to all individuals who have authority to use City electronic communication, Wi-Fi, and IT resources.

II. POLICIES and STANDARDS

<u>Administrative</u>

Any requests to the IT department should be in writing at a minimum and would also utilize the City's ticketing system. Any request that does not utilize the City's ticketing system may not be fulfilled. Any exception to this is in the event of an emergency where no work can be completed such as in the event of a network outage, compromised system, etc.

All employees will be required to sign the Information Technologies Policies and Standards Agreement before using City IT resources. Department directors will be responsible for ensuring this statement is signed and forwarded to Human Resources for placement in the personnel file. Human Resources will thereafter obtain the required signoffs from all new employees hired by the City during employee orientation.

Department directors are considered to be the custodian of all information pertaining to their department as well as enforcement of this policy within their department. Disciplinary action for violation of this policy may include, but is not limited to, verbal or written reprimand, suspension or termination. The department director, together with the City Manager, Human Resources and the IT Director will investigate reported violations to determine if any action is justified.

E-Mail

Scope- Applies to use of City e-mail services by City employees.

Policy-

a) The City of Whitewater is the owner of all e-mail accounts and addresses in its registered domains as well as email accounts created outside of the City's domains for City business. All e-mail messages processed by the City's e-mail server become the property of the City of Whitewater. City of Whitewater e-mail users have no right of ownership or expectation of personal privacy in their e-mail usage.
b) Additional encryption beyond what the City is currently utilizing is prohibited on any documents or e-mail created on City IT resources, without prior approval by the IT Director.
c) The City reserves the right, without notice, to inspect, modify, return, reject, redirect or discard any e-mail message it receives, for any reason. The City reserves the right, without notice, to limit or restrict any individual's e-mail usage.
d) The City may place system-wide limitations on e-mail usage in order to protect the well-being of the City's e-mail infrastructure and ensure system availability and reliability for all e-mail users (e.g., maximum mailbox size, maximum message size)
e) All e-mail messages and attachments are centrally archived and indexed automatically upon arrival to the Exchange Email Server.
f) City e-mail services shall be used in accordance with all applicable Federal and State laws, City ordinances, policies, rules and regulations, and Administrative Instructions, and may not be used as a vehicle to harass or intimidate. All users of City e-mail services are expected to conduct themselves in a professional and ethical manner.
g) City e-mail services are provided for the purposes of study, research, service, and other activities, which must be in the conduct of official business or in support of the City's mission, with the exception of occasional personal use. Personal use shall be kept at a minimum.
h) Access to City e-mail services is granted to an individual by the City for that individual's sole use. Users are authorized to access, use, copy, modify, or delete files and data on their own accounts. Users shall not perform any functions on another user's e-mail account or on a shared mailbox without the explicit permission of the primary user of that account. Users shall not allow someone else to use their account(s) and/or password(s). City e-mail users are responsible for their e-mail accounts and shall be held accountable if someone else uses their service with permission and violates this policy.
i) Subscription to mailing lists, "listservs," or other mass mailings is authorized only when used to conduct official City business. Non-work-related subscriptions to mass mailings are prohibited. The City also reserves the right to unsubscribe any or all City e-mail addresses from said mailings.
j) Access to City e-mail services shall be permanently revoked upon employee termination or retirement. The City shall not forward e-mail messages addressed to terminated or retired City employees except to other City e-mail addresses. The City shall not provide address verification, correction, or forwarding to personal or non-City e-mail accounts or addresses under any circumstances.
k) User privacy is not to be violated. It is the responsibility of the user to protect their privacy. Users shall not leave passwords where they can easily be found, share passwords with others, or leave confidential information on a screen where it could be viewed by an unauthorized person.
l) All City e-mail accounts (and all City digital media) are subject to Wisconsin Open Records Law. While a majority of City records fall under Wisconsin Open Records Law, users should not assume that any message contents or data are automatically subject to public inspection under the Wisconsin Open Records Law. There are exclusions to this law, and such message contents or data may not be forwarded, uploaded, or otherwise transmitted without appropriate approvals.

Internet

Scope- This policy establishes appropriate use of City Internet access for City employees. The City of Whitewater provides employees access to the vast information resources of the Internet with the intention of increasing productivity. While Internet access has the potential to help you do your job faster/smarter, there is justifiable concern that it can also be misused. Such misuse can waste time and potentially violate laws, ordinances, or other City policies.

Policy-

a) City internet access is provided to employees for the purposes of study, research, service and other activities, which, with the exception of occasional personal use, must be in the conduct of official business or in support of the City's mission. Personal use shall be kept at a minimum. This includes the use of the City's Wi-Fi network.
b) Each City employee using the City's internet access shall identify themselves honestly, accurately, and completely when corresponding or participating in online activities.
c) Employees have no right of ownership or expectation of personal privacy as to their City Internet usage. The City reserves the right to inspect any and all network traffic internet usage including Wi-Fi. The City reserves the right, without notice, to limit or restrict any employee's internet usage.
d) Offensive content may not be accessed, displayed, archived, stored, distributed, edited, or recorded using City network, printing, or computing resources. Offensive content includes, but is not limited to, pornography, sexual comments or images, profanity, racial slurs, gender-specific comments, or any content that can reasonably offend someone on the basis of sex, race, color, religion, national origin, age, sexual orientation, gender identity, mental or physical disability, veteran status or any protected status of an individual or that individual's relatives or associates. Any content that may be interpreted as libelous, defamatory or slanderous is prohibited. Exceptions shall be made as it pertains to Police investigations.
e) City internet access shall not be used to conduct personal business, play computer games, gamble, run a business, conduct political campaigns, for personal gain, or to take part in any prohibited or illegal activity.
f) No employee may use City internet access to post a message to an Internet message board, chat room, weblog, listserv, social media site, or other Internet communication facility, except in the conduct of official business. The message must clearly identify the author as a City employee, by name, with the employee's official return City e-mail address or other contact information. Any opinions expressed must include a disclaimer stating that the opinions are those of the author and not necessarily those of the City of Whitewater.
g) Any software or download via the internet may be used only in ways that are consistent with their licenses or copyrights, and only after review and approval by the City's IT Director.
h) No employee may use the City's internet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door, or back-door program code, or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.
i) Internet access from the City's networks is "filtered" using a third-party product/service. Access shall be limited or blocked based upon categories or protocols defined by the vendor of the product/service and the IT Director.
j) Employees requiring access to blocked or limited sites in order to conduct official City business only may request an exemption from a site restriction using their network credentials. This request must be in writing and must provide a specific reason for the override and if the override is temporary. All overrides shall be reported (and are recorded) to the IT Director for review.

Hardware and Software

Scope- Expedite the procurement process for City standard IT equipment. Any standard IT commodity purchase

must be approved by the IT Director or their designee. The City is working to reduce the total cost of ownership of City IT assets.

Policy-

a) Department directors will work with their staff and the IT department to establish appropriate technology implementation and they will consult with the IT department to ensure the equipment is compatible with the City's existing infrastructure.
b) The IT Director or their designee will approve all IT purchases with the exception of peripherals such as keyboards, mice, and speakers to ensure compatibility with current IT resources. This process anchors City IT procurement standards and also promotes cost savings for the City.
c) Installation of hardware and software by persons other than the IT department without prior authorization is prohibited. Employees shall use only hardware and software provided or approved by the City. Any suspected misuse of software shall be reported to the IT Director.
d) All hardware and software inventories will be maintained by the IT department. If a user/department receives hardware or software directly, it will be given to the IT department immediately to be placed into inventory. Web-based applications that do not require downloads or City network resources are exempt from this.

Network

Scope- Applies to all devices connecting to networks owned and managed by the City of Whitewater. The City has made, and will continue to make, a significant investment implementing and information sharing infrastructure to meet the business needs of the City, the work requirements of employees, and the communication needs of the public.

Policy- The following policies are adopted to ensure the internal and external integrity and protection of the City's networks:

a) No non-City owned or managed platforms (PCs, laptops, tablets, or any other devices capable of attaching to the network) will be directly connected through any means to the City's internal networks, without prior approval by the IT Director.
b) No remote connectivity or remote-control software (e.g. PC Anywhere, GoToMyPC, etc.) will be used to connect to the City's network in any way unless approved in advance by the IT Director.
c) No wireless device will be connected to the City's internal Wi-Fi network unless approved in advance by the IT Director. An exception is the use of guest Wi-Fi for personal devices.
d) All platforms approved by the IT Director for connection to the City's internal networks will have the City's anti-virus and antimalware protection software.
e) User names and passwords created by the IT department shall provide internal network access. The requirements for complexity and formatting of these credentials will follow Microsoft's best practice policy for strong authentications. Users are not permitted to place personal passwords on local settings (e.g. screensavers).
f) All users shall log off of the network when they are away from their computer for any significant length of time and when they leave for the day. Per security policy, if the user's computer remains inactive for more than 15 minutes, the connection to the network will be locked. The user will have to unlock their workstation upon return to access the system. Users are responsible for properly safeguarding any administrative data such as logins and passwords, and are held accountable for any activity which occurs under their login name and password. Users must log off when they are not immediately near their workstation.
g) All personal and shared workstations must be restarted at least once a week.

h) Anti-virus and antimalware software shall be loaded on all servers and workstations, and all programs, files, external storage devices, downloads, etc. are actively scanned during usage. If a user finds that any virus, corruption or damage has occurred, or is being reported, contact the IT department immediately.
i) All of the City's servers and information contained therein shall be backed up on a daily basis. Backup media shall be stored in a secure, locked location on City premises and is managed by the IT department. Additionally, the media should be stored off-site in a secure facility at a minimum once per week and ideally in a cloud storage environment. Media no longer used or needed shall be disposed of in the appropriate manner to ensure that data is not retrievable from the discarded media. Users are strongly encouraged to store data in the appropriate folders that are on the City servers so that it is not lost. Any data not stored in designated areas is not the responsibility of the City should it be lost or damaged.
j) Electronic documents will be treated the same as paper documents with respect to City Ordinances (refer to City Municipal Code Chapter 15: Public Records Management) and Resolutions, Regulations, Administrative and Executive Instructions, and Schedules regarding document retention and disposition.

Phone, Fax, Cellular Phone, Photocopy Machines & Other Equipment

Scope- This policy ensures City telecommunications resources are used appropriately. City telephone equipment, cellular telephones, fax machines, photocopy machines, and equipment as outlined below are provided for official City business use only. As such, absent a clear and convincing exception, all landline, cell phone and fax numbers paid for with taxpayer dollars are to be made available to the public on request. City employees are reminded that all messages, calls, files and user actions are subject to monitoring.

Policy-

a) With the exception of occasional personal use, all use of City telecommunications equipment and services is for City business use only. Personal calls should be made during an employee's break or lunch hour, except for necessary work-related situations such as unanticipated overtime or family emergencies. In the event the City is charged for a personal call, the employee may be required to reimburse* the City for the actual cost.
b) City copiers are intended for business use. In the event that an employee uses this equipment for personal use, the employee shall reimburse the city for the actual cost of usage, and personal use shall be kept at a minimum. *
c) Directory assistance (411) calls should be kept to a minimum. Telephone directories are readily available throughout the City and online for outside numbers.
d) City employees that require cellular telephones to perform their essential job functions will be enrolled in a "calling plan" considered to be appropriate for their City business needs. Employees that are issued a cellular phone will sign the City Cell Phone Usage Agreement, and will abide by the rules set forth in the agreement.
e) Voice mail is for business purposes and all messages received are the property of the City. Messages should be deleted from the voice mail system as soon as possible. The City's voice mail system will automatically delete messages after 15 days.

*** Note: The actual cost of usage will be available on the respective City bill and reimbursement for personal usage can be set up through the Finance Department. It is the employee's responsibility to disclose personal use.**

Resource Usage

Scope- This policy applies to all data utilizing City IT Resources. The City has and reserves the right to monitor, review, audit, intercept, access and disclose all information created, received or sent on City IT resources. Information contained in the IT resources will only be disclosed to the extent permitted by law, for business purposes, or as needed to enforce the policy. Authorized access to employee IT resources by other employees or outside individuals

includes, but is not limited to, the following:

a) Access by the IT Director during the course of system maintenance or administration, investigation or network slowdown, system hardware or software problems including software license compliance, general system failure, litigation, or potential litigation.
b) Access approved by the employee, the employee's supervisor, or an officer of the City when there is a need to perform work or provide a service when the employee is not available.
c) Access approved by the employee's supervisor, the City Manager, or an officer of the City when there is suspicion of a crime or violation of a policy.
d) Access approved by the City Manager or the City Attorney in response to the City's receipt of a court order or request from law enforcement officials for disclosure of an employee's e-mail messages.
e) Confidential and misinformation – the release of untrue, distorted, confidential information, or the use of aliases, regarding City business, is prohibited.
f) Equipment, software, hardware or related peripherals are not to be removed from City premises without authorization from the IT Director and appropriate Department directors.
g) The IT department does not monitor employee productivity without explicit permission from the Human Resources Manager, the City Manager, or their designee.

III. JOB AIDS – Form on Next Page

I acknowledge that I have received, read, and understand the City of Whitewater's Information and Technologies Policies and Standards. I understand that failure to comply with the policy could result in disciplinary action up to and including termination of employment. I understand that if I have any questions, I should contact my supervisor, department director or Human Resources.

Employee Signature _____

Employee Name _____

Date _____