DRAFT

Acceptable Use Policy

Acceptable Use Policy

Background and Purpose

The purpose of this document is to define acceptable use of the technology and information resources of City of Manitowoc. This policy applies to all workforce members as well as contractors who use or access City of Manitowoc technology or information resources.

Inappropriate use of organization technology or information resources could expose the City of Manitowoc to productivity losses, security risks, and possible legal liabilities. It is the responsibility of all users of City of Manitowoc technology and information resources to understand and acknowledge this policy and to conduct their daily activities in accordance with this policy.

Components of this policy include:

- Data Classification – See City of Manitowoc Municipal Code
- Roles and Responsibilities
- Monitoring
- No Expectation of Privacy
- Ownership of Information/Equipment and Proper Use
- Information Sharing
- Messaging and Internet Activities
- Incidental Use
- Removable Media Use – Removable Media Policy Ver 1.0
- Encryption
- Hardware/Software Installation and Licensing
- Copyright
- Clear/Clean Desk
- Document and Media Destruction
- Password Use – See 2019-09-27 (MPU) Administrative Safeguards. docx
- Remote Access
- Other Prohibited Activities
- Security Awareness
- Visitor and Guest Access
- Enforcement
- Technology Acceptable Use Policy Acknowledgement (form)

DRAFT

Data Classification

The City of Manitowoc has developed a system of data classification to help ensure protection of organizational and customer information. This allows employees and contractors to appropriately identify, classify, and handle information. At this time the policy and procedure have not been presented to council for formal approval. Until formal approval has been given all data requests shall be referred to the City Attorneys Office. Requests can be sent to cityattorney@manitowoc.org.

The sensitivity guidelines below will be followed when filing and handling information internally to protect information at varying sensitivity levels. Use these guidelines as a reference, as each category may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the information in question.

Public - Information that has been declared public knowledge by statute, the City Attorneys or City Human Resources Office. One does not need a user ID or password nor employment status to access this information. This type of information can freely be given to anyone without any potential damage to the City of Manitowoc, citizens, or customers and no extra caution is required for handling of public information.

Sensitive - Information consisting of valued City of Manitowoc data, this includes Confidential Unclassified Information (CUI). Examples of this type of data include City of Manitowoc proprietary or strategic information, customer lists, customer artwork, blueprints, organizational procedures or internal use only documents requiring a medium level of protection. Compromise of sensitive information could result in financial loss or reputational harm to the organization and workforce members are required to take appropriate actions to protect sensitive information. Additional protections, including encryption, should be considered for electronic transmission to parties outside the organization.

Confidential – Confidential Information consists of information that is highly valuable and mission critical organization or customer information. Examples include Non-Public Personal Information (NPPI) such as Social Security Numbers, trade secrets, tickets, codes, passes, and/or proprietary/critical data of customers. The compromise of confidential information could result in serious harm to the organization in terms of financial, legal, regulatory, and reputational consequences and extreme care must be taken whenever handling Confidential Information. *Encryption is required for electronic transmission to parties outside the organization*.

Roles and Responsibilities

All users are required to securely maintain and operate City of Manitowoc technology and information resources. This includes abiding by all policies detailing Cyber Security requirements. Additionally, users must take an active role in Cyber Security by reporting suspicious activities (such as unusual

computer/system events and anything that appears abnormal from normal daily activities) to supervisors and managers, or directly to the Information Technology Manager.

Workforce members in many cases act as the first line of security defense for City of Manitowoc technology or information resources, therefore all workforce members must participate in the security awareness program. This includes training upon hire, annual training, and recurring awareness activities.

At no time is confidential information (as defined above), or 3rd party information (e.g. artwork, sensitive information or printed material) be stored or transmitted in an unprotected fashion or used for non-business-related purposes. Refer to the *Encryption Policy* if you need further details on how obtain access to the appropriate tools necessary to perform these actions.

Confidential or sensitive information belonging to City of Manitowoc, business partners, customers, or vendors may not be electronically transmitted outside the organization without proper and adequate steps being taken to ensure that:

- All necessary measures and procedures are in place to protect the information and to maintain its confidentiality, including the use of encryption in transmission and at rest where appropriate.
- The information is the minimum needed by the intended recipient(s) for a legitimate business purpose.
- In the case of proprietary information assets belonging to a customer or vendor, releasing this information for its intended purpose is subject to verification for appropriateness in light of any confidentiality agreement or any other agreement between City of Manitowoc and the owner of the information assets.
- Ensure the information is only directed to an authorized recipient(s).

Monitoring

Because the organization is the owner of all technology and information resources, no expectation of privacy exists, and City of Manitowoc management reserves the right to monitor and/or log user's use of these resources with or without prior notice. By accessing organization technology or information resources, users consent to this monitoring. City of Manitowoc will monitor computers and networks to ensure that software and systems are being used in an appropriate manner and that no unacceptable use of computing resources is occurring. City of Manitowoc will report illegal conduct and cooperate with any law enforcement agency if monitored content indicates illegal activity has occurred.

No Expectation of Privacy

Users of City of Manitowoc technology and information resources should not at any time have any explicit or implicit expectation of privacy. For the protection of the organization and workforce members, the organization at any time may examine City of Manitowoc technology or information resources or intercept, monitor, review, and share data with authorized personnel and law enforcement (if necessary). Users are reminded that even deleted information may also be retrieved.

DRAFT

Ownership of Information/Equipment and Proper Use

All electronic information created, sent, received, or stored on resources owned, leased, administered, or otherwise under the control of City of Manitowoc is the sole property of City of Manitowoc. This information is neither personal property nor private, rather it is owned exclusively by City of Manitowoc. There is no expectation of ownership or privacy of data by individual workforce members or users, even if the data has been created by individuals or copied to organization systems from other sources. Users shall not remove, destroy, or modify files or electronic information without authorization. Only approved IT staff may "wipe" information resources. Workforce members must not retain City of Manitowoc information owned by the organization, in any form, after their employment has ended.

All City of Manitowoc technology resources provided to users are for the sole purpose of conducting organization business. Technology and information resources remain City of Manitowoc property at all times. Users are not permitted to copy or otherwise transmit any organization or customer information to unauthorized personally owned devices or services; including, but not limited to, USB devices, external email, or hosted cloud services. Only approved access methods are to be used to access organizational information.

Reasonable methods are to be used by each workforce member or user to keep all technology and information assets protected and in good condition. Modification, abuse, or failure to protect City of Manitowoc technology or information resources from damage or theft may result in disciplinary action.

Information Sharing

Information is only to be shared with approved individuals and organizations, only when required for business purposes, and in accordance with the City of Manitowoc *Data Classification Policy* and contractual obligations. Information is not to be sent to or shared with:

- Unapproved vendors or business partners (those without contracts and agreements for information sharing).
- Non-workforce members, such as friends or family.
- Personal or non-organizational provided email or Internet locations (Gmail, yahoo, dropbox, google docs, etc.).
- Workforce members who do not have a "need to know" about certain information.
- Customers for whom the information does not pertain to or is irrelevant.
- Anyone who does not require it to process or maintain business activities.

Be careful of "over-sharing". Just because a person or company has previously had access to information, does not mean that they still need access to it. Verify agreements prior to sharing, and limit sharing to only what is business relevant at the time.

DRAFT

Messaging and Internet Activities

When using the Internet or messaging services, workforce members are to conduct themselves as "ambassadors" of the organization and must show consideration and respect to others. By default, internet communications should be considered insecure and should not be used for communicating information that requires a high degree of confidentiality without first ensuring the security of the communication (encryption).

Internet activities should primarily be limited to business relevant sites. It is the responsibility of each workforce member to ensure that internet usage is done responsibly and that access to Internet services does not adversely affect productivity or put the organization at risk. Examples of prohibited activities include the following;

- Use of City of Manitowoc technology or information resources to create any inappropriate messages or to access Internet sites that contain inappropriate content. Examples of inappropriate uses or content include, but are not limited to, illegal drugs, gambling, sexually explicit images, ethnic slurs, racial epithets, or any other content a reasonable person would view as harassment or offensive based on race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs.
    - The term “Messaging” shall include, but is not limited to, email, text messages, instant messaging, and social networks.
- Retrieval, interception, or reading of e-mail or other electronic messages not addressed to them, unless expressly authorized by City of Manitowoc or by the message’s original recipient.
- Creating or transmitting un-solicited bulk email (SPAM) is prohibited, unless such activity is defined as part of one’s job responsibilities and conforms to applicable legal requirements.
- Forwarding or in any way participating in e-mail chain letters, scams, or hoaxes.
- Posting to mailing lists, social networking sites, or newsgroups with a corporate e-mail address or other organizational identifier for reasons that are not directly related to your job.

Incidental Use

Incidental, occasional, and limited personal use of City of Manitowoc technology and information resources is permitted during normal business hours, unless prohibited by your supervisor and only to the extent and only for a time period that is reasonable. This includes items such as email, telephones, mobile devices, Internet access, fax machines, printers, and copiers. Information accessed or created on City of Manitowoc resources for personal use purposes is still considered to be the property of the organization and subject to the same conditions, monitoring and restrictions as applied to business use. Incidental use is restricted to organizational workforce members and authorized contractors and does not include family members or others not affiliated with City of Manitowoc. Incidental use is permitted under the following conditions:

- Must not result in direct costs, cause legal action against, or cause embarrassment to the organization.
- Must not interfere with the normal performance of work duties.
- Must not cause noticeable impact or change to operational infrastructure systems, noticeably consume resources, incur support, or otherwise adversely impact the functioning of essential operations.
- City of Manitowoc reserves the right to monitor personal use to ensure compliance with all policies and to determine whether or not it is considered "Incidental Use" at organization's sole discretion.

Removable Media Use

Removable storage devices include, but are not limited to: Universal Serial Bus (USB) devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, MP3 devices, phones, mobile devices and any other existing or future portable computing or storage device that may connect to or access information systems. It is the organization's and workforce member's shared responsibility to ensure that removable storage devices, as well as the information on them, is protected from unauthorized use, access, and theft. To accomplish this, workforce members are to ensure that;

- Devices or media containing confidential or sensitive information are protected using the organization-approved standards, as specified in the *Secure Communications and Encryption Policy.*
- In the event that loss or theft of removable media containing any organization or customer data occurs, the custodian of that media must immediately report this event to the Information Technology Manager and their supervisor.
- Information must be securely removed from removable media in accordance with the *IT Data Destruction and Retention Policy.*

Encryption

Approved encryption methods will be supplied by IT Security and must be used as indicated in the *Data Classification Policy*. Use of unapproved methods may risk sensitive or confidential data, deny valid access to systems, or allow disclosure of data. Encryption settings are not to be tampered with or modified in any way. Workforce members who use removable media, mobile devices, or laptops will be required to encrypt their drives and/or media in accordance with approved policy.

Hardware/Software Installation and Licensing

Only approved hardware and software purchased and installed by the City of Manitowoc Information Technology Services group is authorized to be used on the organization network. Software is not to be downloaded, installed, removed, or modified on City of Manitowoc technology resources without all licensing agreements, security, and authenticity being validated. Software is only to be obtained from authoritative sources. The use of third-party software distribution locations is strictly prohibited (e.g. Download.com or DriverFinderPro.com). Software is always to be obtained directly from the original

manufacturer or creator. In addition, no hardware or software is to be added or removed from City of Manitowoc equipment if it violates any organization policies or state or federal regulations. Periodic inspection (audit) of organization resources will be conducted to verify that only products meeting this criterion have been installed.

Copyright

Software or media copyrights are protected by laws and regulations that protect the rights of content creators. City of Manitowoc supports and upholds the rights of copyright owners by adhering to all applicable laws governing copyrights, trademarks, or brand protection. Violations of copyright laws could subject an individual to criminal or civil penalties. Unacceptable conduct that could constitute violations of copyright laws may include, but are not limited to:

- Making unauthorized copies or distributing copyrighted materials (paper or electronic).
- Providing software or data to any outside party without written authorization.
- Storage, use or download of "pirated" or illegally copied software or media (including images, movies, or audio).
- Use or possession of copyright circumvention tools or codes (e.g., "cracks", "Warez", "Appz", "serials", "keygens", or cheat codes).
- Copying personal software or media (music, videos, books, etc.) to organization technology resources.

Clear/Clean Desk

Workforce members are to adopt a "clear/clean desk" work philosophy. A clear/clean desk does not prescribe cleanliness, but rather describes a workspace that is clear of documents and other materials that are sensitive or contain organization or customer information when unattended.

A clear desk presents a professional appearance and reduces the risk of unauthorized access to information. To adopt this policy, workforce members should consider taking the following actions:

- Cover or store confidential or sensitive documents when unattended.
- Consider the sensitivity of documents before you print.
- Locking desks and filing cabinets at the end of the day.
- Protect devices (laptops, mobile devices, removable media) when not in use.
- Proactively lock your workstation whenever it is unattended.

Document and Media Destruction – "Shred All"

Workforce members are routinely entrusted with various types of media that contains sensitive or confidential customer or business information. These media types may include;

- Paper files and printed copies
- Magnetic and/or solid-state storage media (hard drives, tapes, media cards)
- Flash media storage (portable external or internal storage like USB drives)
- Optical media (CDROM, DVD, Blu-Ray)

City of Manitowoc is responsible for complying with laws and regulations pertaining to the protection of confidential information, recycling regulations, and proper disposal in our facilities. In order to simplify the process of disposal, all paper materials containing confidential or sensitive information, are to be shredded. This includes, but is not limited to, documents, cover pages, sticky notes, note paper and all other paper copies used or generated in the course of business.

Electronic storage media, such as floppy disks, CDs, DVDs, and USB flash drives, are to be destroyed by giving them to Information Technology Services personnel. Destruction of this media is to be performed in accordance with the *IT Data Destruction and Retention policies*.

Only the City of Manitowoc Information Technology area is authorized to facilitate the disposal of obsolete or discarded organization owned equipment. All organization information must be securely removed from all computing devices under the following circumstances:

- After a workforce member terminates their employment
- Before any equipment is discarded
- Prior to sending any equipment to a third-party repair organization

Password Use

Password standards exist to protect the confidentiality, integrity, and availability of our systems. Passwords can be compromised in many ways. To protect against these problems and keep systems secure, workforce member's passwords should follow the *Password Policy* and are to follow these directives:

- Keep passwords from being guessed by making them complex.
- Do not re-use passwords or portions of passwords.
- Do not share your passwords with unauthorized parties.
- Customer and/or organization system passwords are to be shared only with authorized personnel and changed upon termination of an authorized person.
- Do not type passwords on computers that you do not control.
- Protect your password from "shoulder surfing".
- Do not write down passwords or store them digitally in an unencrypted form.

- Do not allow non-City of Manitowoc IT staff to assume un-supervised control of a computer or application to which you have logged in.
- Lock your computer session whenever you walk away from a system. Do not wait for the automatic screen lock timeout.
- If you think a password may be compromised, change it immediately and contact Information Technology Services and your immediate supervisor.

Remote Access

Some workforce members may be granted access to the City of Manitowoc network to work remotely. Only approved remote access methods and devices are allowed to be used to remotely access internal information systems. If a workforce member is approved for remote access, the following restrictions and requirements apply to remote access use:

- Only devices provided by City of Manitowoc are allowed to remotely connect directly to the organizational network or systems.
- Remote access systems are to be used in the same manner as computer systems within City of Manitowoc offices and are subject to the same policies.
- Ensure reasonable physical security is maintained for the computing platform used for remote access.

Other Prohibited Activities

Under no circumstances may a user of City of Manitowoc technology or information resources participate in any conduct that would be considered illegal or otherwise violates organization policy or ethical standards. This includes, but is not limited to, the following:

- Attempting to access or intentionally destroy any data, documents, email correspondence, or programs contained on systems for which you do not have authorization or approval.
- Sending or storing organization or customer information on non-organization owned or managed systems other than with organization-approved methods. Examples of unapproved methods include emailing sensitive or confidential data to a personal email account or storing data in an unauthorized cloud service.
- Use of peer-to-peer file sharing (e.g., Kazaa, eDonkey) for any purpose, including distributing, sharing, sending, or receiving audio, video, or data.
- Using non-organization sponsored messaging programs (e.g., AOL Instant Messenger (AIM), MSN Messenger, Yahoo! Messenger, Skype) to send and receive real-time messages over the Internet.
- City of Manitowoc resources may not be used to engage in activities that would violate the copyright protection of another person or company. This activity includes, but is not limited to, the transmission, storage, copying, distribution, or installation of non-licensed software, artwork, music, videos, content, or images on or using City of Manitowoc resources.
- City of Manitowoc resources shall not be used for the purpose of crypto mining.

- City of Manitowoc resources may not be used to engage in soliciting others for commercial ventures, political or religious causes, outside organizations, or for any other similar solicitation not sponsored or endorsed by the organization.
- City of Manitowoc resources may not be used to play games, gamble, or to sell/purchase/obtain illegal drugs.
- City of Manitowoc technology resources may not be used while operating a motorized vehicle, power equipment, or in areas of operation of such equipment; however, the use of mobile phones while driving is permissible if allowed by law and if hands-free devices are utilized or, if not available, if an workforce member believes a call will be of a type and duration that will not cause a diversion of attention that would be unsafe to the workforce member or others. At no time, while driving, may workforce member's e-mail, text, read messages, browse the web, or conduct any other activity with City of Manitowoc technology resources that diverts attention from the road.
- Attempting to or purposefully introducing malicious software into the organization or its customers computing environment. Malicious software includes any undesired functions and typically includes, but is not limited to, backdoors, viruses, worms, Trojan horses, or Spyware.

The following activities are also prohibited except in cases where they must be conducted for legitimate reasons by authorized technology staff in the course of their duties who have obtained prior written approval from City of Manitowoc IT Security:

- Providing or share username and/or password with unauthorized persons. This includes family members, co-workers, and supervisors. Organization staff (IT resources) will **never** call or email to ask the workforce member for his or her password. Any attempt to do so should be immediately reported to the Information Technology Manager.
- Attempting to access City of Manitowoc resources that you are not authorized to access.
- Circumventing, or attempting to circumvent, any security restrictions or settings that govern proper use. This includes, but is not limited to, the use of proxy avoidance software, disabling system settings, or use of any improper or modified connection settings, password crackers, networking sniffing, spoofing of network traffic, and denial of service attacks, port scanning, or any other manner of manipulating normal flow of technology or information.

Security Awareness

Technology and information resource users are required to complete the mandatory security training and are requested to review any additional material when made available. At a minimum, this will happen at hire and annually thereafter.

Visitor and Guest Access

All contractors are required to display visible company issued identification on entry into non-public areas of organization facilities.

Workforce members are to advise visitors about connecting their computing devices to the organization's authorized visitor technology resources. All City of Manitowoc facilities have a "guest" wireless network to provide Internet access to visitors. Visitors computing devices are not allowed to connect to organization non-guest network resources without prior approval from the Information Technology Manager or their designee.

Enforcement

Unauthorized or inappropriate use of technology or information resources by any user could result in the loss of, or limitations on, the use of resources, or disciplinary and/or other adverse actions. These actions may include actions up to and including termination of employment. In addition, criminal penalties may also result.

If you become aware of any misuse of City of Manitowoc technology or information resources, or noncompliance with organization policies, please report this immediately to your supervisor or to the Information Technology Manager.

1. Revision History:

Version	Date Modified	Modified By	Details
1.0			Initial policy