



City of Waukesha

IT Acceptable Use Policy

- I. **Purpose.** This Acceptable Use Policy serves as an agreement between the City and any User of Information Technology (IT) assets. Any use of IT Assets is deemed to be an agreement by the User to abide by this Policy, and a violation of this Policy may subject the User to disciplinary action. Any questions about its terms or interpretation should be directed to IT.
- II. **Definitions.** For purposes of this Policy, capitalized terms have the following meanings:
- A. **Device** means without limitation any desktop computer, laptop computer, notebook computer, tablet, mobile phone, smart watch, USB flash drive, external hard drive, external optical-disk drive, SD card or any-other portable data-storage media, monitor, display, printer, hot spot, hub, wireless access point, physical or virtual server, switch, firewall, physical or virtual gateway, router, security sensor, camera, or any other equipment that is able connect in any way with, communicate data of any kind through, or use in any way IT Assets, defined below; whether owned by the City or any other entity or individual.
 - B. **IT** means the City of Waukesha Information Technology Department.
 - C. **IT Assets** means City-owned, -leased, or -controlled property, whether tangible or intangible, that is used in any way in connection with the generation, collection, processing, storage, transmission, reception, communication, distribution, or other use of analog or digital data. Without limitation, IT Assets specifically include telephone, internet, email, text, wireless, video, audio, radio, satellite, mobile, and all other digital or analog communications equipment and infrastructure; data; software; software-as-a-service; applications; cloud storage services; cloud applications; virtual computing platforms; fiber-optic and metallic-wire networks and related facilities; local-area networks, wide-area networks; web sites; social-media sites; IP addresses; URLs; internet domains; peripherals; all City-owned, -leased, or -controlled Devices; and any structures in which any of these items are housed or stored.
 - D. **User** means any individual who operates a Device or uses IT Assets, regardless of whether that individual is a City employee or not. Without limitation, User includes vendors, independent contractors, agents, and members of the general public.
- III. **Applicability.** This Policy is applicable to all Users.
- IV. **User Responsibilities.**
- A. Users shall use only Devices, software, apps, and services that are pre-approved by IT.
 - B. All IT Assets are on loan to Users so that essential job functions may be performed.
 - C. Upon separation from the City or contract termination, all supplied IT Assets, and the associated data shall be returned by the User.
 - D. Users shall secure the physical environment around their workstation and lock their computers when stepping away.
 - E. Users shall ensure that personally-identifiable information and confidential or sensitive data that may be subject to protection by law is not available to or accessible by unauthorized persons.

City of Waukesha

IT Acceptable Use Policy

- F. All Users shall take appropriate care to protect information, systems and related assets within their custody or care from loss, damage, or harm.
- G. Lost or damaged equipment shall be reported to IT as soon as possible.
- H. Users shall store their passwords in a secure manner. Passwords cannot be written or printed on paper and left where they can be easily found or discovered, and they cannot be stored in an unencrypted form, such as an Excel spreadsheet.
- I. Only password managers that are pre-approved by IT may be used to store passwords digitally.
- J. User-assigned accounts shall only access assets, operating systems, applications, files, and data to which they have been expressly been granted permission to access. The ability inadvertently to read, execute, modify, delete, or copy data does not imply permission to do so.
- K. Only Users authorized by their Department Head are permitted to post content or create the impression. All postings are subject to the City's Media Protocol and Social Media Protocol, which take precedence over this Policy.
- L. All communications with the media are subject to the City's Media Protocol and Social Media Protocol, which take precedence over this Policy.
- M. Users shall keep knowledge about information and information systems gained during employment confidential and confidentiality shall be maintained after employment ceases.

V. Prohibited Uses.

- A. Only devices that are pre-approved, authorized, and issued to Users by IT may be connected to City networks and other IT Assets. This includes portable end-User devices, removable devices (e.g., USB sticks) and personally-owned devices. Other devices may be connected to IT Assets only with express pre-approval by IT.
- B. Users shall not share their passwords with others or allow the use of their accounts by others.
- C. Users are responsible for all activity originating from their Usernames and accounts.
- D. Users shall not circumvent User authentication mechanisms or the security of any User account or information system asset.
- E. Users shall not install software or hardware, or modify system configuration settings, on any IT Asset without the express permission and oversight of IT.
- F. Users shall not engage in any activity with the intent of disrupting IT Assets or networks.
- G. Users shall not perform any form of network monitoring, port scanning, or security scanning unless this activity is a part of the User's regular job duties and is expressly authorized by IT.
- H. Users shall not use IT Assets for personal economic gain.



City of Waukesha

IT Acceptable Use Policy

- I. Users shall not leverage the “Remember Me” or “Remember my Password” function within a browser.

VI. Expectations of Privacy

- A. When using City resources, the User shall have no expectation of privacy. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by law.
- B. The City reserves the right to monitor, access, and disclose all information generated and actions performed using City IT Assets. Files, messages (including attachments), and logs may be retained and used as evidence in litigation, audits, and investigations.

VII. Personal Use

- A. Users are permitted limited personal use of IT Assets, such as visiting websites and checking personal email accounts, subject to all other City Work Rules.
- B. Users may access web-based personal password managers on IT Assets, but shall not store City-related passwords in them. Local installation of a password manager must be pre-approved and performed by IT.
- C. Users shall not store City passwords in personal password managers.
- D. Users shall not use browser sync or browser profiles that will move a User’s browser history from a personal device to a City asset or vice-versa.
- E. Users shall not use personally-owned accounts (e.g., Apple ID, Google Account, Microsoft Account) for device-wide accounts (e.g., Android, iOS, Windows) on City devices.
- F. Users shall work with IT to create City-specific accounts for required assets and third-party services, such as creating a City-owned Apple ID for an Apple device.
- G. Users shall not use City license keys on personal devices unless expressly pre-authorized by IT.
- H. City data shall not be stored on non-City, personal cloud provider platforms (e.g., Google Drive, Dropbox).

VIII. Reporting Threats. Users who are aware of any event which threatens the availability, integrity or confidentiality of City data, or which breaches any standard, policy, procedure, or any associated requirement, or is contrary to law, shall immediately notify IT or their immediate manager.

IX. Remote Work. When conducting City work remotely, the following rules apply to all Users:

- A. All City work shall be performed on City-approved assets.
- B. All City data shall be stored on approved IT Assets.
- C. Users shall not connect IT Assets to open, unencrypted Wi-Fi networks.
- D. Users must be aware of their surroundings when working remotely to ensure others are not shoulder surfing or viewing sensitive material.



City of Waukesha

IT Acceptable Use Policy

X. Bring Your Own Device

- A.** Personal devices shall not be connected to the City network without express pre-approval from IT.
- B.** City data shall not be stored on personal devices without express pre-approval from IT.
- C.** Users leveraging their personal device to store City data may have their device completely wiped. Reasons for device wipe may include:
 - 1.** Lost or stolen device.
 - 2.** Termination of User's employment.
 - 3.** Compromised or hacked account or device.

XI. Exceptions. Departments requesting any exceptions from the terms of this Policy shall provide a request to the IT Director. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk upon granting the exception, risk mitigation measures to be undertaken by IT, initiatives, actions and a time frame for achieving the minimum compliance level with the policy set forth herein. The IT director shall review such requests and confer with the requesting department.

XII. Penalties for Violations. Violations of these rules will subject the User to discipline, up to and including termination, as provided in Human Resources Policy G-3.

Passed by the Information Technology Board on the 5th day of March 2025.

Approved by the Common Council on the 11th day of March 2025.

Shawn N. Reilly, Mayor

, City Clerk