



City of Albany
Administrative Policy
Policy #: IT-001-001
Title: Technology Usage

**Information
Technology**

Purpose This policy is meant to provide employees and managers with an understanding of the proper usage of City technology systems.

Policy This policy is applicable to all employees.

- Technology systems and Internet access provided by the City are to be used for official City business functions. They are not to be used for personal purposes except as outlined in this policy. The City will not be responsible for personal items that are damaged, lost, or stolen. *Employees are hereby notified that they shall have no reasonable expectation of privacy when using any items listed in this paragraph.*
- Any use of City technology in the course of City business that degrades, humiliates, or embarrasses any person is strictly prohibited. This includes, but is not limited to, any degrading comments based on race, sex, age, religion, national origin, disability, or any other protected class.
- The proper use of technology systems is an important method of securely and effectively carrying out the City's mission. Like other City assets, these systems are acquired to help City employees carry out their job responsibilities efficiently. Technology systems will be procured, installed, and secured in accordance with CIS and NIST cybersecurity guidelines and frameworks.
- Information created, stored, sent, or received by City employees in connection with City business, or using City assets or facilities, which includes technology systems and most forms of electronic media devices, may be public record. See "Archiving of Public Records" - ORS 192.005 and "Inspection of Public Records" - ORS 192.311 and 192.314 for the definition of a public record. Public records may be subject to disclosure under Oregon public records law. Public records are subject to the Oregon secretary of state's retention schedule. Employees should not make public disclosure decisions. Employees should contact the records and information management (RIM) coordinator for their department or the city clerk's office in the event that they receive a public records request.

A. Internal Network

- 1) The City's internal network is comprised of core network infrastructure, systems, and services upon which the City relies to conduct critical operations. Connections to the City's internal network are not permitted without prior authorization from the information technology department.
- 2) Connections to the internal network are closely provisioned and monitored to ensure a secure environment. Employees will obtain IT authorization prior to



moving a device on the internal network or connecting a new device or service to the internal network. This is in order to maintain security and an accurate inventory in compliance with the cybersecurity policy and the City's insurance requirements.

B. Workstation Security

- 1) Employees will lock or log off the workstation while it is unattended.
- 2) Employees will log off the workstation and leave it powered on at the end of their shift to facilitate maintenance and security updates.

C. Usernames and Passwords

- 1) Employees may not share usernames or passwords used to access City technology systems. Exceptions, which require IT authorization, may be permitted if the use of shared accounts is required to efficiently conduct business.
- 2) Employees may not reuse or copy, either whole or in part, City passwords on other sites or services.
- 3) Passwords may only be stored in an encrypted electronic format.
- 4) Multifactor authentication is required for all domain user accounts.

D. Training


- 1) Employees are required to complete initial and recurring technology security training as outlined in the cybersecurity policy.

E. Purchasing

- 1) IT authorization is required prior to the purchase of a device or service, if the device or service connects to the internal network and/or IT personnel will be required to install, manage, or secure the device or service. This is to ensure efficient use of limited central services personnel, compatibility with City systems and security requirements, and to evaluate proper retention of public records in the new systems and legacy systems. As a cost-saving measure this also allows IT to determine if the functionality is already being provided or if there is a superior or more cost-effective alternative. Additionally, IT awareness prior to the purchase of the device or service is critical to ensure that existing vulnerabilities can be properly resolved or mitigated.

F. Personal, Sensitive, or Confidential Information

- 1) It is the responsibility of each user to comply with the cybersecurity policy to

	<p>City of Albany Administrative Policy Policy #: IT-001-001 Title: Technology Usage</p>	<p>Information Technology</p>
---	---	---

prevent unauthorized access to and distribution of personal, sensitive, or confidential information.

G. Third-party Access

Any third party that requires access to the internal network must agree to the relevant agreement(s) before access can be allowed, and the access must be approved and managed by IT in accordance with CIS and NIST guidelines. Evaluations will be performed on third parties to ensure that they are adhering to relevant agreements. Agreements can include, but are not limited to:

- 1) Network and/or VPN access.
- 2) Access to technology systems containing personal, sensitive, or confidential data.
- 3) CJIS or HIPAA compliance.

Third-party access agreements will be managed by the IT department and limited in duration.

H. External Access

- 1) External access to the internal network is permitted only for devices or services that have been authorized by IT, to include any VPN connection.

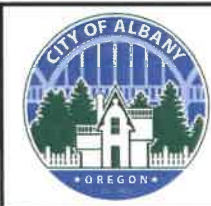
I. Loss or Theft

- 1) If a City-owned device is lost or stolen, the user will contact the Help Desk immediately and file a police report.
- 2) IT Critical Response will be contacted immediately at 541-286-7517 if the loss or theft occurs outside of normal business hours.

J. Prohibited Activities

The following activities involving City technology systems are prohibited:

- 1) Exploiting, or attempting to exploit, a vulnerability or circumvent security measures (hacking).
- 2) Sharing information with others that may facilitate unauthorized access.
- 3) Transferring personal, sensitive, or confidential data to any removable or portable device unless access to that information is within the scope of the user's job and the data or device is encrypted in accordance with the cybersecurity policy.
- 4) Transmitting or storing personal, sensitive, or confidential data unencrypted.



- 5) Providing personal, sensitive, or confidential data to unauthorized users.
- 6) Leaving personal, sensitive, or confidential data exposed to view while unattended.
- 7) Opening email attachments from an unknown, suspicious, or untrustworthy source.
- 8) Gaining, or attempting to gain, information for criminal purposes or for any purpose outside the scope of the user's job.
- 9) Gaining, or attempting to gain, user account or password information that belongs to others.
- 10) Connecting an unauthorized device to a City technology system.
- 11) Installation or execution of unauthorized software.
- 12) Web usage that significantly impacts network integrity, security, or availability.
- 13) Any computer crime as defined by Oregon Revised Statutes (ORS) 164.377.

K. Telework Systems

The City may provide the employee with a telework (VPN) system for the purpose of working remotely. In addition to the policies above, the following policy also applies to telework systems:

- 1) Telework systems will not be assigned until a telework agreement has been approved by the user's department director and the HR director, and the approved telework agreement has been provided to IT and a VPN user agreement is on file with IT.
- 2) No applications or services on the telework system will be installed or modified unless authorized by IT.
- 3) Personal use or storage of personal files on the telework system is prohibited.
- 4) The user identified in the telework agreement is the only user authorized to use the telework system.
- 5) The user will take delivery of the telework system from IT at city hall.
- 6) Upon request, the user will return the telework system to IT at city hall within 72 hours (e.g., for maintenance).



City of Albany
Administrative Policy
Policy #: IT-001-001
Title: Technology Usage

**Information
Technology**

- 7) The telework system will only be assigned for the duration specified on the telework agreement.
- 8) The user will return the system to IT at city hall within 72 hours of the expiration of the telework agreement.
- 9) If the telework system is no longer needed, the user will return the system to IT at city hall within 72 hours.
- 10) To ensure compliance with the cybersecurity policy, only City-issued workstations may be used for remote work.

L. Telephone Usage (Non-mobile)

- 1) Long distance calling should be used prudently since each minute is billed to the City.
- 2) Employees may not make personal long-distance calls using the City's long-distance service, even if the employee reimburses the City for the costs of these calls.
- 3) Employees should use extra care in making local personal calls that do not have extra toll charges connected with them. Frequent or protracted personal conversations take away from productive work time. Abuse of work time is subject to disciplinary action. Expressly prohibited is the use of City telephone systems for carrying out non-City business, trade, advertising, and/or selling personal or non-City business items.

M. Mobile Devices

- 1) City employees who use mobile devices for City business use the devices with different frequency, varying from occasional use to frequent use. Given the variations, the purpose of this policy is to provide for flexible, cost-effective use of mobile devices. It is the City's intent to minimize the number of City-provided mobile devices to the fullest extent possible.
- 2) To maintain compliance with the Oregon records retention law, employees who are issued a City-owned device or receive a mobile device allowance are required to use the Microsoft Teams Chat application on the device to communicate information related to official City business. Please see Appendix A for examples of messages that do and do not have to be retained.
- 3) All employees are asked to exercise caution when deleting any messages. Please contact your department RIM coordinator if you are uncertain if a message should be retained or deleted.
- 4) Should you accidentally send a message related to official City business from a



City of Albany
Administrative Policy
Policy #: IT-001-001
Title: Technology Usage

**Information
Technology**

private device, or a messaging application that was not Microsoft Teams, please forward it to your cityofalbany.net email address where it can be archived.

- 5) Use of a mobile device while operating a vehicle on City business must be performed in accordance with current applicable Oregon law and motor vehicle codes.
- 6) The following options are available to City of Albany employees who use mobile devices for City business:
 - a. Mobile devices supplied by the City.
 - (1) Employees with a daily business need for a mobile device may be assigned a City-issued mobile device.
 - (2) Use of a City-issued mobile device is restricted to City business. Personal calls (outgoing or incoming) will only be allowed infrequently for limited duration in emergencies when these calls cannot be made from a land line or personal mobile device within a reasonable period of time.
 - (3) City-issued mobile devices will be City property, on a connectivity plan provided by the City, and administered by mobile device management infrastructure.
 - b. Mobile device allowance provided as an employment benefit.
 - (1) The City recognizes that, due to the nature of some positions, it may be more cost-effective and give more flexibility to provide some employees a mobile device allowance in lieu of providing the employee with a City-owned mobile device.
 - (2) Under this plan, managers may designate employees who will be provided with a monthly allowance to obtain a personal mobile device.
 - (3) Under this plan, the employee is allowed unrestricted business and personal use of his or her cellular telephone.
 - (4) Employees who receive a cellular telephone allowance are responsible for obtaining their own device and usage plan.
 - (5) Employees who receive a cellular phone allowance may seek separate reimbursement from the City for excessive charges incurred for a specific emergency situation with the approval of their department director.



City of Albany
Administrative Policy
Policy #: IT-001-001
Title: Technology Usage

**Information
Technology**

(6) Employees who receive a cellular phone allowance may be required to install software or access network resources on the device in support of City business.

c. Employees who carry personal mobile devices that are rarely used for City business shall submit an expense reimbursement form to cover business use charges.

N. Email and Voicemail

- 1) Email is provided as a communication avenue for City business. Email is considered a public record, and all messages sent by email should be viewed in this light. Any message or wording that degrades, humiliates, or embarrasses any person is strictly prohibited. Employees should periodically review their email and appropriately delete messages that are no longer germane to operations. Emails are subject to public records retention requirements, and employees should contact their department's RIM coordinator or the city clerk's office for retention schedule information. City email accounts will only be issued to City employees.
- 2) Voicemail is assigned to City employees based on the need to enhance telephone communications with internal and external customers. Voicemail allows callers to leave messages for City staff members. Employees should not leave messages which should not be shared with any other person. As with email, employees should periodically delete voicemail messages that are no longer germane to operations.

O. Personal Use

- 1) Technology systems are intended to be used to carry out official City business. Employees are not to use these systems for non-City or personal work unless given prior approval by their supervisor. Employees are prohibited from using these systems for profit-making ventures or businesses.
- 2) Copiers and Facsimile Machines. These may be used to produce limited numbers of personal copies or faxes, provided they are not for a non-City, profit-making business and provided the employee records the number of copies made, faxed, or received as a fax and reimburses the City at the prescribed rate. Personal long-distance faxes are prohibited.
- 3) Workstations. Department directors may authorize the use of workstations and related office equipment for personal use of a limited duration on non-work time for training or development purposes if it is intended to increase employee work skills, produce a usable product pertinent to City operations, or maintain a professional certification pertinent to the employee's job with the City. ***Employees are hereby notified that they shall have no reasonable expectation of privacy for any information created, stored, received, or sent***



on City technology systems. Individual hard drives and any electronic media devices are subject to inspection by supervisors and IT staff under the direction of the HR Director and the IT Director. Personal use must comply with the other restrictions and prohibitions spelled out in this policy. Use of City workstations for carrying out a non-City business, trade, advertising, and/or selling personal or non-City business items is prohibited.

Information created, stored, sent, or received on the City's internal network may be considered a public record. Public records may be subject to disclosure unless the record or material is exempt under Oregon public records law. If material is exempt from public disclosure, then it may be stored and labeled as "Confidential." However, it is the content of the material and not its storage location or designation as confidential which would allow the City not to disclose the information. Should a request be made for information within an employee's confidential directory, then the city attorney will determine whether the specific material requested falls within one of the exemptions.

- 4) Software. Management and IT department approval is required for employees to install personally owned software on City computers. Directors, managers, and supervisors may install demonstration software to evaluate programs for City use. Copying of City-owned software is prohibited unless explicitly approved by management and allowed under software license requirements. All managers shall check with the IT department before approving installation of personal software or copying of City-owned software.

P. Internet Use

- 1) Employees are given access to the internet to perform their work assignments. The internet must not be used for personal profit or entertainment by any City employee.
- 2) The internet is a worldwide network of interconnected computers containing billions of pieces of information and many diverse points of view. Employees are responsible for the material they access and obtain from the internet. All internet use by City employees on City equipment is monitored and subject to periodic review.
- 3) Employees will not view, send, receive, print, or otherwise disseminate materials that degrade, humiliate, or embarrass any person. This includes but is not limited to any degrading materials or information based on race, sex, age, religion, national origin, or disability. Sexually explicit materials may not be viewed, archived, stored, sent, received, distributed, edited, or recorded using a City technology system. Users are to report inappropriate use of the internet through the City's system to their supervisor, department manager, or human resources.



City of Albany
Administrative Policy
Policy #: IT-001-001
Title: Technology Usage

**Information
Technology**

- 4) Anything created or viewed by City employees on the internet will be treated as a public record and archived as specified by public records rules. Confidential and/or sensitive information should be avoided unless it is a prescribed function of the user's job.
- 5) All files and data received from the internet or from computers or networks that do not belong to the City must be scanned for viruses and other destructive programs. Files that are attached to email leaving the City's network should also be checked for viruses.
- 6) *Employees have no expectation of privacy as to their use of the Internet through the City's network.* The City has the right to monitor any sites employees visit on the internet, including web pages, chat rooms, and news groups. Human resources may authorize information technology to review internet activity and analyze usage patterns of employees at any time. The City may choose to distribute this data to the management staff.
- 7) Employees must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property and online activity, including downloading of any copyright protected computer programs. Questions regarding licenses, copyrights, and intellectual property should be directed to information technology staff.
- 8) Employees are not to use the internet for non-City or personal work unless given prior approval by their supervisor. Any personal use must comply with all aspects of this policy. No use will be made of the internet by an employee for a profit-making venture or business or for any political use prohibited by Oregon law. Personal use of the internet should take place only during nonworking hours, should be infrequent, and should not be a substitute for an employee obtaining private internet access. Frequent or protracted personal use of the internet is prohibited. Personal use of the internet during work time or use of the internet that has not been authorized by an employee's supervisor is subject to disciplinary action.
- 9) Certain exceptions to this section may be permitted to Albany Police Department employees as a function of the employee's assignment with the express approval of a supervisor.

Q. Summary

- 1) The proper use of City technology systems enhances productivity and security, which allows the City to better meet increased service needs while decreasing risk and liability. Proper use of technology systems also ensures compliance with legal requirements. It is the responsibility of each employee to use these systems in an appropriate manner. Violation of this policy or procedures set forth in this document may be grounds for disciplinary action.



The City may temporarily suspend, block, or restrict access to technology systems in accordance with the cybersecurity policy.

Definitions

CIS – the Center for Internet Security, a non-profit organization that publishes IT best practices and cybersecurity frameworks.

Connection – is a communication channel across which data is transmitted between technology systems.

Device – is any equipment item, peripheral, or accessory that can execute software and/or store, process, or transmit data.

Electronic Mail (Email) – is a service designed to allow users to send and receive communications.

External Access – is any connection from outside the City’s internal network to the City’s internal network.

Internal network – is any technology system that can only be accessed on-premises or via virtual private network (VPN) connection.

NIST – an agency of the US Department of Commerce that develops standards, guidelines, and best practices to manage cybersecurity risk.

Personal, sensitive, or confidential data - is:

- i. Personally identifying information (PII) such as social security number, home address and home phone number
- ii. Credit card and bank account numbers
- iii. Criminal history information subject to CJIS
- iv. Personal health information subject to HIPAA
- v. User account and password information

Public Record – information created, stored, sent, or received by City employees in connection with City business, or using City assets or facilities, which includes technology systems and most forms of electronic media devices, may be public record. See “Archiving of Public Records” - ORS 192.005 and “Inspection of Public Records” – ORS 192.311 and 192.314 for the definition of a public record.

Service – a platform, either local or remote, to include cloud services and third-party providers, that provides a technology service in support of business operations.

Technology system – a platform comprised of a device, or devices, that provide for the processing, integrity, security, storage, transport, or management of data in support of business operations.

Voicemail - is any recorded message made on the City’s telephone system and



City of Albany
Administrative Policy
Policy #: IT-001-001
Title: Technology Usage

**Information
Technology**



includes both incoming messages and the prerecorded greeting to callers.

Workstation- is a personal computer connected to the City's internal network.

References

Human Resources Policy Ethics
Archives Division's Administrative Rules (Chapter 166)
F-05-08, Public Records Request
F-06-08, Records Management Policy

Review and Authorization

Supersedes: HR-ER-13-006 08/01/2013	Created/Amended by/date: SP; 06/21/2021	Effective Date:
IT Director: 	City Manager: 	

1. Form or worksheet revision related to this document? No Yes

If yes, attach a copy of the revised form or worksheet.

2. Training required? No Yes



City of Albany
Administrative Policy
Policy #: IT-001-001
Title: APPENDIX A

**Information
Technology**

The below information is intended to assist employees in making sound decisions about their use of messaging technology.

Text messages

Work-related communications sent and received via text message are subject to the same retention requirements as those sent via email, fax, or paper. This applies whether the device in use is agency-issued or privately owned. City employees cannot avoid public records laws by using a privately owned device. However, not all messages are of equal value. Transitory records do not need to be retained. An example of a transitory record is a record documenting routine activities containing no substantive information, such as routine notifications of meetings and scheduling of work-related trips and visits.

Transitory messages that do not need to be retained include:

- “John, can you work overtime this Tuesday to repair the flux capacitor at the plant?”
- “Sue – I’m attaching photos from the pipe today that did not pass inspection.”
- “Can you bring out a load of rock to the job site?”
- “What are you having for lunch?”
- “I need help with the pumps at this lift station. Can you send Fred out?”
- “Sally has called in sick for tomorrow. Can you cover her shift?”
- “Look at this cute cat video I found!”

Messages that communicate official City business and do need to be retained include:

- “I plan to ask City Council to award the project to Aperture Science.”
- “The inspection is complete. All work was found to be in compliance and the permit is approved.”
- “I told the vendor they could have three more months to complete the project.”
- “I told the customer we would discount their service by 25 percent.”

When considering whether a message should be retained, it is helpful to ask:

- 1) Does this message convey information of a decision made regarding official City business; and
- 2) Is this message the only copy of this information?

If the answer to both questions is yes, the message must be retained.

Instant Messaging in Microsoft Teams

Messages sent via Microsoft Teams are subject to the same retention requirements as those sent via text, email, fax or paper, and have the same retention exceptions as noted above for text messages. The retention of Teams messages is managed automatically in accordance with the City’s retention schedule.