AUHR 4.08 INFORMATION TECHNOLOGIES

Purpose

The City of Portland provides information technologies to its employees to use in the course of doing their jobs. This administrative rule covers the use of information technologies for internal and external communication as a tool for conducting the City's business, and as a research tool and information resource. The term Information Technologies includes, but is not limited to, computer and telecommunications hardware, software, and systems that utilize the Internet and/or any other communications network.

This administrative rule mandates ethical employee use of information technologies, encourages use that enhances employee productivity, confirms that electronic communications used in the conduct of government are generally considered public records and prohibits inappropriate use.

The Bureau of Technology Services (BTS) maintains authority for the technical rules and standards of information technologies and the City Auditor maintains authority over Auditor's Office employee behavior in the use of those technologies.

Because of the rapid change in information technologies, this administrative rule will be reviewed periodically and modified to address new concerns.

Employee Use of Information Technologies

Auditor's Office employees' use of City information technologies must comply with all applicable Oregon Revised Statutes, City Code and City or Auditor's Office Administrative Rule provisions. Auditor's Office employees must comply with accepted standards and practices for use.

Employees' use must protect the integrity of the City's computer systems, data and networks. Employees' use of information technologies must comply with all service and contractual agreements with commercial Internet service providers, intellectual property rights, copyright and software license agreements.

Documents, emails and other electronic records created using the City's information technologies are public records and may be subject to disclosure. They must be preserved in compliance with City record retention and preservation policies. Accessing the City's internal networks from employee owned computing devices such as employee owned home computers, or any portable computing device (such as a laptop, smartphone, or other electronic device used to access electronic data) may subject the employee's personal

devices to disclosure. When conducting City business using any personal computing device including a home computer or portable computing device, employees and City Officials should always use City email.

All employees using City information technologies are responsible for reading and complying with this administrative rule.

No Expectation of Privacy in the Use of Information Technology

All computer applications, programs, and information created or stored by employees on City owned information systems are City property**. Employees shall have no expectation of personal privacy in the use of the City's information technologies.**

Passwords are used to protect the security of City data and information technologies and are not intended to convey an expectation of personal privacy or exclusion from monitoring.

Auditor Rules May Be More Restrictive

The standards and guidelines outlined in this administrative rule are minimum standards for City bureaus and offices. The Auditor's Office may develop rules regarding office-specific use of information technologies. The Auditor's Office may develop more restrictive work rules based on operational needs in consultation with BTS. All drafts of specific IT work rules must be forwarded to the BTS Chief Technology Officer (CTO) for final review prior to implementation.

Monitoring and Reporting of Information Technologies' Usage by the City of Portland

The City of Portland monitors the use of information technologies including e-mail, website visits, other computer transmissions and any stored information created or received by City employees with the City's information systems. Monitoring may result in reports logging usage and printed or electronic copies of email or stored information.

Use of the City's information technologies constitutes an express consent to monitoring at all times.

The City makes an effort to block access to certain Internet content deemed by the Bureau of Technology Services information security manager to be of high risk to the City network and users. This content is typically one that has the potential to deliver malware to the City's network and/or users or is inappropriate. If content is blocked because it is inappropriate that determination will be made in consultation with the City Auditor.

Requests for monitoring and reporting of City technology use, including but not limited to the Internet activity or e-mail use of an individual employee or division and monitoring and reporting of video/audio recording of an employee must be submitted in writing to the City Auditor or designee and must be submitted by a division director. These requests may include, but are not limited to monitoring the inappropriate use of information technology, the fulfillment of public records requests, or the electronic discovery of evidence for actual or potential litigation in which the City is an affected party. Nothing in this section requires the City Auditor's approval for routine monitoring of telephone calls and other activities for quality control purposes.

Individual Reports

Requests for monitoring a specific employee's technology use should contain a reason for the request.

Group Reports

Requests for aggregate reports for group or office-wide technology use do not require a specific rationale.

Neither individuals nor groups need to be notified of monitoring. However, should the report indicate use of information technologies, which violates Auditor's Office or City Administrative Rules, all applicable requirements in a collective bargaining agreement or in the administrative rules must be followed prior to implementing discipline.

Generating Reports

When the City Auditor approves a monitoring request, a written request defining the desired information will be submitted to a designated Bureau of Technology Services (BTS) staff member. BTS will generate a report and submit it to the City Auditor. The Auditor's Office and BTS will maintain a record of all requested reports.

Confidentiality

Reports on individual technology usage are considered personnel information and should be viewed as confidential. Electronic content may also be confidential for other reasons and will be reviewed in a manner to protect that confidentiality and to comply with all applicable laws. However, these reports are public records and may be subject to disclosure. All requests for disclosure should be referred to legal counsel for response.

Website Blocking Exception

The City Auditor acknowledges that on occasion, there may be a legitimate and compelling City business reason for an individual or a specific work group to gain access to Internet content that is otherwise blocked. If such a situation arises, a division manager must submit a written request to the City Auditor which includes:

1. The name and position of the employee(s) for whom an exception is being requested;
2. The specific web site, category of sites, to which the employee(s) require access;
3. The compelling business need for access to the content.

The City Auditor, in consultation with the Bureau of Human Resources, will review the request and provide a written response. The Auditor's Office is predisposed to maintaining a consistent policy on Internet access and may suggest alternative approaches for meeting the business need. The City Auditor shall work with the Bureau of Technology Services to determine if such a request is technically feasible. If the request is technically feasible, the City Auditor will send authorization and written instructions to a designated Bureau of Technology Services staff member requesting that the exception be implemented.

Acceptable Use of Information Technologies

The City's information technologies are intended for professional business use in performing the duties of an employee's job. All employees who use the City's information technologies have the responsibility to:

1. Protect City technology assets.
2. Select, use and secure strong individual passwords for access to system accounts (e.g. for network login, email, desktop computer) and never share access accounts, privileges and associated passwords.
3. Accept accountability for all activities associated with the use of their user accounts and related access privileges. For shared devices each user is responsible for their own use.
4. Ensure that use of City information technology, including computers, devices (including mobile devices), email, internet access, computer accounts, networks, and information stored or used on any of these systems, is restricted to authorized purposes.

5. Report all suspected security and/or policy violations to an appropriate authority (e.g. manager, supervisor, BTS Helpdesk, Information Security Manager).

6. Support compliance with all federal, state, and local statutes and regulations and applicable industry requirements.

7. Follow all applicable BTS Administrative Rules, and all specific policies, guidelines and procedures established by the Auditor's Office as well as agencies with which they are associated and that have provided them access privileges.

Unless otherwise prohibited by law or specific work rules, limited personal use is permitted according to the following guidelines;

1. It is incidental, occasional and of short duration;

2. It is done on the employee's personal time. Personal time means during breaks, lunch and/or before and after work as defined by collective bargaining agreements, Administrative Rules and Auditor's Office work rules.

3. It does not interfere with any employee's job activities. This includes activities which might pose a conflict of interest or appearance of impropriety with an individual's employment with the City or the Auditor's Office;

4. It does not result in an expense to the City;

5. It does not solicit for or promote commercial ventures, religious or political causes, outside organizations or other non-job related solicitations;

6. It does not violate the other "Prohibited Uses" section in this administrative rule;

7. It does not disrupt the Bureau of Technology Services' ability to provide information technology services to City users;

8. Personal use must meet the requirements of this rule and an individual's personal use can be denied by their division manager due to operational or other concerns.

Other acceptable uses of information technologies include:

1. Communication with other federal, state or local government agencies, their committees, boards and commissions;

2. Communications, including information exchange, research, professional development or to maintain job knowledge or skills;

3. Communications and information exchanges directly relating to the mission and Charter of the City of Portland and work tasks in support of work-related functions.

Prohibited Use of Information Technologies

The following list of prohibited uses for information technologies is not intended to be all-inclusive.

1. To cause a breach of security or any action to attempt to circumvent or reduce the security of the City's computer and network resources or of any confidential information, regardless of physical or electronic form or media, entrusted to the City's custody.
2. Misuse of service or any action that renders the user's computer equipment unusable, or that interferes with another City employee's use of information technologies.
3. Illegal use or use of any City information resources, regardless of physical or electronic form or media, for any use including but not limited to the commission of an illegal act.
4. To grant or allow personnel access by any person or entity to City information technology systems or data, regardless of physical or electronic form or media, for which they are not authorized to do so.
5. Failure to limit the recipients of messages appropriately, propagating virus hoaxes, "spamming" (spreading e-mail or postings widely and without good purpose), or "bombing" (flooding an individual or group with numerous or large e-mail messages).
6. Accessing or transmitting information that conflicts with City Code, Administrative Rules or Auditor's Office work rules for non-job-related reasons such as information in violation of the City's non-discrimination policy.
7. Accessing racist and sexually explicit sites.
8. Commercial endorsement or use of City information technologies in a manner that would constitute an endorsement of a specific commercial entity, its products, services, or business practices. Neither the City's e-mail system nor the City's intranet may be used for commercial activities, religious causes, or support for other activities that are not related to the direct conduct of city business. An exception may be permitted if such information is central to a bureau's mission and meets stated Auditor's Office goals and objectives. The exception must be pre-approved by the

City Auditor. Authorized employee discounts may also be posted in a specific “employee only” section of the City’s web portal.

9. Use of City information technologies for political activity or in a manner that would directly or indirectly assist a campaign for election of any person to any office, or for the promotion of or opposition to any ballot proposition. This prohibition shall not apply to the use of City computer or network resources for the development or delivery of a neutral and objective presentation of facts relevant to a ballot proposition as allowed by state law, provided that such use must be a part of the normal and regular conduct of the employees developing or delivering the presentation of facts.
10. Altering electronic communications to hide one’s identity or to impersonate another individual. All e-mails, news posts or any other form of electronic communication must contain the sender’s real name and/or e-mail address.
11. Buying, selling or trading goods, services or financial instruments via the City’s information technologies for personal financial gain.
12. Using software that allows a workstation or other City of Portland information resource to function as an unauthorized, unmanaged server.
13. Using City information technologies to avoid the expense of personally purchasing comparable hardware, software, and/or internet access.
14. Removing City owned IT equipment from City premises (except as specifically allowed by the user’s manager, such as taking home a City owned laptop computer for City business), modifying (beyond normal parameters of use) City owned IT equipment, or altering City owned software without appropriate written authorization from the Bureau of Technology Services.
15. Installing any software not previously approved by the Bureau of Technology Services including unlicensed software. This does not include downloading and installing properly licensed and approved software from BTS maintained systems.
16. Copying and/or using City data, regardless of physical or electronic form or media, for personal use, except as permitted by law.
17. Destroying City records in violation of retention and preservation policies

Broadcast or "All Employee" E-Mail Messages

Employees may not use the City's e-mail system to send "broadcast" e-mail messages outside of the Auditor's Office unless there is City Auditor approval. In this instance "broadcast" means sending an e-mail message to 50 or more City employees.

To send a broadcast e-mail to all employees, the sender must have the endorsement of the City Auditor and follow procedures established by BTS for "All City Employees" email messages, including but not limited to including the following warning: **"Please do not use the Reply to All function to respond to this message. The appropriate contact person is listed in the message.** The sender must contact the BTS HelpDesk for authorization to use the "All City Employees" distribution list. Broadcast messages containing attachments will be reviewed for file size.

The City's web portal may be the most appropriate place for announcements of general interest.

Union Use of E-Mail

Union use of e-mail is authorized in accordance with the above stated section on

Acceptable Use of Information Technologies provided it does not conflict with bureau work rules and the section on "Prohibited Use".

Malware Protection

The Bureau of Technology Services is responsible for assuring that City-approved anti-malware protections are installed, maintained, and active on all computers. Employees are expected to take all malware warnings seriously and to comply with procedures for reporting and responding to malware outbreaks. Deliberate transmission of data containing malware or willfully circumventing malware protection measures will be considered a breach of security and in violation of this rule.

Technology Rules and Standards

For Technology Services Administrative Rules, go to https://www.portlandoregon.gov/citycode/index.cfm?&c=26821

For Technical Standards, go to: http://www.portlandoregon.gov/bts/46940

Electronic Records Retention and Preservation

With few exceptions, any electronically stored information, regardless of electronic form or media that pertains to City policies, decisions, transactions and activities is subject to public disclosure and record retention and preservation requirements.

1. Transitory records

   Records of short-term interest (90 days or less), which have minimal or no documentary or evidential value. Included are such records as:

   - Routine requests for information or publications and copies of replies which require no administrative action, no policy decision, and no special compilation or research for reply
   - Originating office copies of letters of transmittal that do not add any information to that contained in the transmitted material
   - Quasi-official notices including memoranda and other records that do not serve as the basis of official actions, such as notices of office parties, holidays or charity fund appeals, and other similar records
   - Records documenting routine activities containing no substantive information, such as routine notifications of meetings, scheduling of work related trips and visits, and other scheduling related activities
   - Listserv messages
   - Fax confirmations
   - Reading materials
   - Reference materials
   - FYI e-mail information that does not elicit a response
   - Unsolicited advertising

   Emails that fall under the Transitory category should be deleted from the e-mail system by the user as soon as any operation or informational value has expired.

   Note: Calendars for elected officials and bureau heads must be retained permanently and calendars for other city employees must be retained for one year.

2. Correspondence

   Records that directly relate to City programs, management or administration. These include but are not limited to formal approvals,

directions for action, communications about contracts, purchases, grants, personnel, etc.; and correspondence relating to a particular project or program.

Records that fall under the Correspondence category must be managed as an official City record in a suitable storage environment.

Contact Information

Technical questions regarding the use of information technologies should be directed to the Bureau of Technology Services. Any human resources related issues should be directed to Management Services.

Human Resources Rule Information and History

Questions about this administrative rule may be directed to the Management Services Division of the Auditor's Office.

Adopted by the City Auditor December 11, 2017.

Adapted from City of Portland Human Resources Administrative Rule 4.08 Information Technologies.

Adopted by Council March 6, 2002, Ordinance No. 176302.

Last revised April 25, 2016.