Metro | *Policies and procedures*

Subject Information Technology: Acceptable Use

Section Information Services; Human Resources

Approved by Martha Bennett, Chief Operating Officer; MERC Commission

POLICY

Information, computer systems and devices are made available to users to optimize employee productivity in support of Metro's business processes. The purpose of this policy is to inform technology users of the appropriate and acceptable use of information, computer systems and devices.

Applicable to

All employees and other users of Metro agency information-related technology, services or systems.

Where provisions of an applicable collective bargaining agreement directly conflict with this policy, the provisions of that agreement will prevail.

Definitions

Access: To instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system or computer network.

Computer Software: Computer programs, procedures and associated documentation concerned with the operation of a computer system.

Encryption: Use of a process to transform data into a form in which the data is unreadable or unusable without the use of a confidential process or key.

Information System: Computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with access beyond ordinary public access to, Metro's shared computer and network infrastructure.

Technology Asset: A data processing device that performs logical, arithmetic or memory functions, including the components of a computer and all input, output, processing, storage, software or communication facilities that are connected or related to such a device in a system or network. Technology assets include, but are not limited to, computers, tablets, telephones, and other messaging devices.

Technology Services: Information systems that are functioning on the public network subscribed to by Metro, including services found on the Internet that hold and process mail, files or streams of information.

Users: All Metro employees, volunteers, vendors and contractors who access Metro information assets, and all others authorized to use Metro information technology for the purpose of accomplishing Metro's business objectives and processes.

Guidelines

1. **Users have no right to expect that any information created on, kept on, or transmitted through the Metro information system is private.**
   a. All information created or kept on Metro information systems, including email, is subject to review for compliance with public records law, regardless of whether the content is business-related or personal.
   b. Metro documents, communications and work products stored on personally owned devices are also subject to public records law. The use of personally owned electronic devices such as home computers, laptops, smart phones and tablets to access Metro's internal networks may subject the personal device to review and possible disclosure.
   c. Metro may monitor all electronic communications and information contained on its systems. Metro may monitor any and all email traffic passing through its email system as well as website visits, other computer transmissions, and any stored information created or received using Metro's information systems.
   d. Metro will disclose or maintain the confidentiality of information in accordance with applicable law.
2. Metro information systems and devices are provided for business purposes only; however, Department Directors may approve limited, incidental personal use consistent with the terms of this policy.
3. Metro expects employees to comply with normal standards of professional and personal courtesy and conduct in their use of email and other electronic communications.
4. The Information Services Department is responsible for issuing guidance, consistent with this policy, to address changing technology or business needs. At a minimum, newly issued guidance will be posted on the IS intramet page and notification will be emailed to employees with Metro email addresses.
5. Violation of terms of this policy may result in the limitation, suspension or revocation of access to Metro information systems and can lead to other disciplinary action up to and including termination.

Procedures

General security protocols

1. All users must be authorized by Information Services to use Metro technology assets.
2. Users are responsible for the security of their passwords and accounts. Users must keep their passwords confidential. Passwords must be changed on a regular basis and should be complex enough that they cannot be easily discovered.

3. Users of Metro information systems shall respect the confidentiality of other users' information. Users shall not attempt to:
    a. access third-party systems without prior authorization by the system owners;
    b. obtain other users' login names or passwords;
    c. attempt to defeat or breach computer or network security measures;
    d. intercept, access, or monitor electronic files or communications of other users or third parties without approval from the author or responsible business owners;
    e. review the files or information of another user without a specific business need to do so.
4. **Remote access:** Users may access Metro networks and email from remote locations only with proper authorization and through the use of agency-approved and agency-provided remote access systems or software.
    a. Telecommuting is subject to applicable Metro policies and collective bargaining agreements.
5. **Software:** Non-approved software, including but not limited to desktop and workgroup applications, screen savers, browsers, application plug-ins and games, may not be downloaded or installed from the Internet, portable computer and storage devices, or other external sources without prior approval from Metro Information Services.
    a. Approved software is listed on the IS Department intramet page.
    b. Employees who have an ongoing business need to download non-approved software may request an exception from the requirement to obtain prior approval each time. Such requests must be supported by the employee's supervisor and submitted to the IS Department in writing. IS will evaluate the request with due consideration to the employee's business need, Metro's operational readiness, and the potential security impact. If the request is granted in whole or in part, IS will provide a written description of the expanded approval.
    c. The IS Director has final authority over software approval decisions.
6. **Privately owned electronic devices:** Privately owned devices may not be connected to Metro networks, wireless access points, computers or other equipment without prior approval from Metro Information Services.
    a. Privately owned devices such as laptops, smart phones and tablets may be connected to the email server over the public internet in accordance with IS Department guidance.
    b. Hardware devices that are not required for assigned work must not be attached to a Metro-provided computer. All hardware attached to Metro systems must be appropriately configured, protected and monitored so it will not compromise Metro technology assets.
7. **Instant messaging and streaming video/audio:** Departments may allow the use of Instant Messaging (IM) and other communications or messaging alternatives for business purposes. Departments may also allow the use of streaming video/audio for business purposes. However, these uses must be approved, documented, and adequately secured and must comply with Metro records and information management policies. The IS Department is authorized to monitor IM communications and video/audio streams as needed for business or legal reasons.

8. Technology assets must not be used in a manner that impairs the availability, reliability or performance of Metro business processes and systems or unduly contributes to system or network congestion.

9. Users are required to report evidence of computer viruses, security breaches, or unauthorized access to the IS help desk as soon as possible.

10. Metro-provided email systems and Internet access for the public must be secured appropriately in order to protect Metro technology assets.

11. Metro may employ additional security controls, such as limited workstation access, in order to protect Metro technology assets and maintain a secure environment.

12. Information Services is responsible for monitoring the use of information systems and assets. At a minimum, IS will monitor on a random basis and for cause. Monitoring systems or processes will be used to create usage reports and the resulting reports will be reviewed by Information Services management for compliance.

Restriction of personal use of Metro technology assets

13. Internet use increases the risk of exposing Metro technology assets to security breaches. Metro can only accept this risk for business uses.

    a. Business use includes accessing information related to employment with Metro, such as accessing benefit-related information. Approved sites for this purpose are the Oregon Public Employees' Retirement System (PERS), Employee Assistance Program (EAP), Oregon Savings Growth Plan and union contract information.

    b. Department Directors may determine whether to allow limited incidental personal internet use, such as to check weather conditions or in case of emergency.

    c. Metro has discretion to determine if an employee's use is personal or business. Employees will not be disciplined for personal use without an opportunity to explain any business reasons for the use.

14. Email is to be used for Metro-related business only, except as follows:

    a. Department Directors may allow employees limited, incidental personal use as long as it does not violate other requirements of this policy and there is no significant cost to the agency.

    b. Email may be used for union business to the extent allowed in the applicable collective bargaining agreement.

15. Metro employees are responsible for exercising good judgment regarding the reasonableness of personal use of Metro's technology assets. No personal use of Metro information systems shall interfere with staff productivity, pre-empt any business activity, consume more than a trivial amount of resources, or be used for personal gain.

    a. Users may not use Metro technology systems to play computer games, regardless of whether Internet-based, personal, or included with approved software applications.

    b. Metro systems may not be used for hosting or operating personal Web pages; non-business-related postings to Internet groups, chat rooms, or list services; or creating, sending or forwarding chain emails.

c. Metro information systems, other than the intramet bulletin board, may not be used for personal solicitation. Systems may not be used to lobby, solicit, recruit, sell or persuade for or against commercial ventures, products, religious or political causes, or outside organizations.

Prohibited uses

16. Metro networks and systems shall not be used to intentionally view, download, store, transmit, or retrieve any information, communication or material that:

    a. is harassing or threatening; is obscene, pornographic or sexually explicit;

    b. is defamatory;

    c. fosters hate, bigotry, discrimination or prejudice or makes discriminatory reference to race, age, gender, sexual orientation, gender identity, religious or political beliefs, national origin, health or disability;

    d. is untrue or fraudulent;

    e. is illegal or promotes illegal activities;

    f. is intended for personal profit;

    g. facilitates Internet gaming or gambling; or

    h. contains offensive humor.

17. Under certain circumstances, there may be legitimate business reasons to access materials that are otherwise prohibited. Employees should obtain supervisor approval before accessing such materials.

18. Users shall not intentionally destroy data in an attempt to misrepresent data in Metro information systems.

19. Personal hardware or software may not be used to encrypt any Metro-owned information except with express prior permission and direction from Information Services.

20. Users shall not send email or other electronic communication that attempts to hide the identity of the user or represent the user as someone else. Users shall not utilize proxy devices or servers to hide their identity or to circumvent existing security. No use of scramblers, remailer services, drop-boxes or identity-stripping methods is permitted.

Additional legal requirements

21. All information created on or stored within Metro's applications, systems, devices and networks, whether on or off-premises, is the sole property of Metro and subject to its sole control, except as required by contract. In addition, all Metro documents, communications and work products are the sole property of Metro, regardless of whether the information is stored, accessed or transmitted via Metro-owned or personally owned devices such as computers, tablets, and cell phones.

    a. No part of Metro agency systems or information is or may become the private property of any system user.

    b. Metro owns all legal rights to control, transfer, or use all or any part or product of its systems.

c. Metro is under no obligation to store or forward the contents of an individual's email inbox, outbox or contact list either during or after their employment.

22. Use of Metro information systems must comply with copyrights, licenses, contracts, intellectual property rights and laws associated with data, software programs and other materials made available through those systems.
23. Users must comply with Metro's records retention policies.

Responsibilities

Employees:

- Take reasonable steps to ensure the physical security of Metro technology assets and passwords and report missing, lost or stolen Metro technology assets to their supervisor immediately.
- Use Metro technology assets in a manner consistent with the Acceptable Use Policy, seeking answers to any questions about the policy from their supervisor or the IS help desk as needed.

Supervisors:

- Ensure that authorized users have received training on acceptable use through the Metro Learning Center software or have received and signed a hard copy of the policy.
- Submit new account request forms for new employees.
- Review and update employee access when requested.
- Ensure employees are using Metro technology assets in a manner consistent with the Acceptable Use Policy and guard against inappropriate use of such assets by employees.
- Coordinate with the agency's Information Services and Human Resources Departments on violations of acceptable use of Metro technology assets.

Department directors:

- Ensure that department purchases for Metro technology assets are restricted to only those necessary for the conduct of official business and that standards for hardware and software are followed.
- Ensure appropriate usage of Metro technology assets and compliance with applicable rules and policies.

Information Services:

- Implement firewall, anti-virus, role provisioning, password controls, web surfing and Email filtering mechanisms, ensure their maintenance, and monitor logs and reports for system performance and compliance.
- Report policy violations to the Human Resources Department and/or supervisory staff as appropriate.

- Create hardware and software standards with the help of a technical standards committee and publish hardware and software standards on at least an annual basis.
- Review policy annually to determine applicability. Publicize new guidance on the intramet and by email.
- Update filters by employee or group to include items required as part of the job when directed by a manager.

<u>Human Resources Department:</u>

- Alert Information Services of policy violations when appropriate.

Related References

- Information Services Department intramet page:

  http://imet.metro-region.org/index.cfm/go/by.web/id=3265
- Social Media policy