600 NE Grand Ave.
Portland, OR 97232-2736

www.oregonmetro.gov

Metro | Policies and procedures

Subject Information Security
Section Information Services
Approved by Martha Bennett, Chief Operating Officer; MERC Commission

POLICY

Metro recognizes digital information as a valuable asset necessary to its operations. The purpose of this policy is to establish the processes and procedures, and educate employees, about keeping Metro's information systems secure.

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

1. 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.
2. Computer Software: Computer programs, procedures and associated documentation concerned with the operation of a computer system.
3. Customer Confidential Data (confidential data): This is private information provided directly or indirectly by Metro customers that is necessary for fulfillment of services provided by Metro. This includes private consumer information such as cardholder information, names, addresses, telephone numbers, etc., and account numbers, information about individual accounts, or any other information that can be individually tracked to a consumer or customer. Card Holder Information (including Primary Account Number or PAN) is ALWAYS considered "Confidential" and should be secured accordingly. Breaches of confidentiality may violate state or federal law, or third party legal agreements.
4. 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.
5. 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.

6. Metro Confidential Data (confidential data): This is data or information kept by Metro that relates to its financials, personnel data, legal matters, technical specifications, or other information that could significantly harm Metro or its employees, if it is not adequately protected. Breaches of confidentiality may violate state or federal law, or third party legal agreements.
7. Mobile Devices: Electronic devices used for mobile communications including mobile telephone, email, text messaging or data transmission, over a cellular network. In addition to the standard voice function, cellular devices known as smartphones and/or tablets may support many additional services and accessories, such as application software (third-party "apps"), text messaging, email, internet access, camera and GPS. Additionally, cards for the purpose of providing cellular network access (this type of card requires some type of monthly service plan) for mobile computing devices such as a laptop are also considered a cellular device.
8. 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.
9. 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.
10. Users: All Metro employees, elected officials, 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. Departments working with Information Services (IS) are responsible to protect the confidentiality, integrity, security and availability of technology assets, customer and Metro confidential data, information systems, and technology services; this includes all payment card industry (PCI) data (soft and hardcopies) and systems.
2. Each user has a responsibility to protect the confidentiality, integrity, security and availability of technology assets, customer and Metro confidential data, information systems, and technology services. Therefore, it is important for users to be aware of security policies and procedures and reinforce these policies in interactions with others in the workplace.
3. Immediately after hire, and annually thereafter, each employee must affirm their commitment to information security by reading this policy and signing the acknowledgement form. The acknowledgement form is retained in each employee's permanent record.
4. Password Protection: All information systems will be password protected. IS will activate automatic password protection systems where possible. Users are

required to use passwords to protect those devices and activate them on devices without automatic password protections such as smartphones.

5. Confidential Data: Users working with and having access to confidential data are responsible for helping to ensure its confidentiality. IS is responsible for working with departments and as appropriate users to establish and implement systems to ensure the security of confidential data.
6. Confidential data requires strong security controls to prevent unauthorized access or modification of the data. Unauthorized access or disclosure of this level of data can result in significant legal, regulatory, or reputational damage to Metro.
7. All users are subject to and must comply with the provisions of the Information Systems: Acceptable Use Policy, and other policies as applicable, in addition to the provisions of this policy.

PROCEDURES

1. IS will develop further procedures for implementing the provisions of this policy and post them on its MetroNet page.

Password Protection and User Account Security

2. Employees must log off or lock all workstations (e.g., PCs and laptops) at the end of the day and at any time the employee is not in immediate control of the workstation (for example, if you leave your desk for any reason).
3. IS will enable and manage automatic password protected screen savers on all Metro workstations, mobile devices and cellular phones to prevent unauthorized access. The screen saver must automatically activate after 15 minutes of inactivity.
4. To ensure the security of Metro's information systems and applications, and to comply with numerous regulations and standards, users need to follow a strict password management protocol established by IS for accessing Metro's technology assets. Compliance with these policies is mandatory and will be automatically enforced by IS where possible.
5. Users are responsible for changing passwords whenever their passwords are reset by the IS help desk.
6. After a minimum of six failed logon attempts, accounts will automatically be locked out for a minimum of 30 minutes (or until an administrator enables the account).
7. Users must protect their passwords and must not reveal them to anyone. At no time will an authorized employee ask for a user's password. The use of group or shared passwords or other authentication methods by users is specifically prohibited.
8. Passwords must not be written down or stored unencrypted by users.
9. Users are responsible for changing their password and notifying the Help Desk should there be any suspicion the password has been compromised. Examples of potentially compromised passwords include stolen devices, passwords used on systems/devices that have been hacked, suspicious activity on a system, etc.

10. Users may not allow their Metro computers to be used by anyone other than Metro employees. Family and friends may not use Metro computers.
11. On public access computers provided by Metro, IS will implement measures to ensure personal data entered into software programs, such as job application systems, is appropriately secured.

User Identification

12. Users will be assigned a unique ID before they are allowed to access business system components and or any systems containing payment card data.
13. System access for users will be assigned for each system based on the individual's job classification and function and the user's role in the system. Restriction of access will be dependent upon the least access necessary to perform job responsibilities. All role and system access assignments must have documented approval (electronically or in writing) by authorized parties. Roles will be regularly reviewed and updated.
14. Physical access to sensitive areas will be authorized based on job function and shall be revoked immediately upon termination.
15. User's access will be deactivated or removed immediately upon termination.
16. Any user accounts that have been inactive in the past 90 days will either be removed or disabled.
17. No user will be provided with direct access to queries and/or databases except database administrators.

Confidential Data

18. Confidential data, is to be secured and protected while in transit over networks and while in storage per directions from IS.
19. The requirements to encrypt confidential data stored on electronic media vary depending on the sensitivity of the data and how the data is accessed and/or used. Departments are responsible for initiating requests for IS to assist them with encrypting and securing confidential data. IS will work with departments and users to ensure that these requirements are met based on the type of confidential data being accessed and/or used.

Electronic Media

20. Confidential or sensitive information must never be copied onto removable electronic media or removed from secured Metro facilities without authorization from the Department Director or IS.
21. Electronic media containing customer confidential or sensitive data must be stored securely, labeled as confidential and be physically retained, stored or archived only within secure Metro locations, subject to Metro's records retention schedules or third party agreements.
22. All media must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked and that have been approved by IS.

Sharing Data with Service Providers

23. If cardholder data is shared with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), the following policies and procedures must be followed:
24. Operations must maintain a documented list of any service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network.
25. Any written agreement with a service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network, must include an acknowledgement of the service providers' responsibility for securing all cardholder data they receive from Metro.
26. Prior to engaging with a service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network, Metro will conduct due diligence and follow an established process to ensure that the security of cardholder data within the service provider's network has been addressed.
27. Metro will have an ongoing program to monitor the PCI Data Security Standard (DSS) compliance status of any service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network.

Vendor Access

28. Accounts used by vendors to access, support or maintain system components via remote access must be approved by IS prior to use.
29. Such accounts will be enabled only during the time period needed and disabled when not in use
30. Vendor remote access accounts must be monitored by staff when in use.

Employee Facing Technologies

31. Metro has developed use policies for all critical employee-facing technologies (e.g. remote-access technologies, wireless technologies, removable electronic media, laptops, e-mail use and Internet use). Employee use of employee facing technologies under this policy, including cellular phones and mobile devices must comply with the provisions of the IT: Acceptable Use and Cellular Phone Policies.
32. Explicit management approval is required prior to using any employee-facing technology in the cardholder data environment.
33. Any employee-facing technology used must be authenticated with a user ID and password or other authentication item (for example, token).

Cloud Computing and Approved Cloud Storage Providers (CSPs)

34. Cloud computing resources may only be used for business purposes and with the written approval of the IS Director. CSP access is granted for specific use based on user job duties and business need.

35. Acceptable CSPs are those that have been approved by IS. IS will publish a list of approved CSPs on its MetroNet page.
36. Users are only allowed to access CSPs using Metro workstations or laptops for approved business needs.
37. Users may not use CSP to store any documents that contain the following:
    a. Social security numbers
    b. Credit card numbers, sensitive authentication data, cardholder names, or expiration dates (collectively and individually known as cardholder data or CHD)
    c. Data protected by HIPAA (electronic protected healthcare information or ePHI)
    d. Personally identifiable information (PII) or financial information (PIFI)
    e. Data that, if advertently exposed to the general public, would cause material harm or bring discredit to Metro or related organizations

Metro Owned Mobile and Cellular Phones/Devices

38. Users with Metro owned mobile or cellular phones/devices must regularly update their cellular phone's operating system to the current version of the software. IS will not support cellular phones that are unable to be updated to a recent version of the operating system software. Users of phones that cannot run a recent version of their operating system should contact IS to arrange for a cellular phone upgrade in order to be in compliance with this Policy and the Cellular Phone Policy.
39. Users must activate the password protection on their cellular phone.

Remote Access

40. Remote access is restricted to users who have a valid business requirement for it. Metro will incorporate 2-factor authentication for remote user access originating from outside the Metro network by personnel and all third parties.
41. Users accessing Metro Webmail or other Metro information systems remotely are responsible for accessing it on a technology service that is running a recent version of its operating system, that is actively employing anti-virus software and have their system password protected.
42. IS is not able to provide support for individual users accessing Metro technology services remotely.

Employee Wireless Access

43. The Metro guest wireless network is provided for business purposes only. Rules for its use are the same as for use of other Metro information systems and devices. Department Directors may approve limited, incidental personal use consistent with the terms of this policy and the IT: Acceptable Use Policy. The Metro wireless network may only be used for business needs subject to supervisory approval. Access to Metro business resources will not be provided through the guest network.

Anti–Virus (Malware) Software

44. Users may not disable or attempt to disable or otherwise circumvent anti-malware systems.

Laptop Computer Security

45. It is employees' responsibility to maintain the physical security of their Metro-issued equipment when out of the office. Theft of equipment should be reported to the IS Help Desk immediately by employees. Employees are required to return Metro-issued information systems upon separation from Metro or when taking an extended leave of absence. When traveling users should not put Metro laptops or other information systems in checked baggage.

Incident Reporting

46. Breach of Security, Virus or Other Security Problem: Users suspecting that a security incident or breach of information systems security has occurred, a virus is on the system, or having concerns about any other security vulnerabilities or issues, should:
    a. Contact the IS Help Desk immediately at x2222;
    b. If off-site call 503-797-2222, or email "HelpDesk" and include the word "Critical" in the subject line; and
    c. After normal work hours, send an email to the "HelpDesk" with a description of the security incident or breach, virus or other concern and in the subject line include the word "Critical." Do not wait until the next day.

Responsibilities

Employees:

- Immediately after hire, and annually thereafter, you are required to read the Information Security Policy and sign an acknowledgement of having done so. Questions about this policy should be directed to the Help Desk.

- Help ensure the security of Metro's information systems by following the password protection procedures in this policy and protocols issued by IS.

- Contact the Help Desk immediately if you suspect a breach of security, a virus or other security vulnerability.

- Any employee who is aware of a potential violation of this policy must immediately report the matter to his or her supervisor and to the IS Director, or to the Human Resources Director.

- Comply with provisions of other applicable policies including the IT: Acceptable Use and Cellular Phone Use Policies.

Supervisors:

- New users: Ensure that new employees are aware of the Information Security Policy.
- Ensure that employees in your unit are following the Information Security Policy.
- Notify Human Resources or IS when employees are transferring to a different work unit to ensure that their access is modified or terminated as appropriate.
- Notify IS when employees are inactive for 90 or more days.

Department Director:

- Is responsible for ensuring that work units with access to or using confidential data are working with IS to ensure the security of the data and information systems where it is maintained, stored and/or transmitted.
- Ensure that this policy is being implemented by supervisors and employees in your Department.
- Report any suspected information systems security issues to the IS Department Director immediately.
- Responsible for department implementing appropriate security systems for maintaining the confidentiality of electronic and hardcopy confidential data, including PAN, and periodically auditing electronic and hardcopy security of that data, including systems for storing and disposing of confidential data.

Human Resources:

- HR will notify IS when employees transfer or terminate. Upon notification of an employee's transfer or termination, information systems services must ensure that the user access is disabled.

Information Services:

- Will implement technology solutions designed to help Metro departments comply with this policy.

- Will issue and post on the MetroNet password protection protocols.

- Responsible for auditing information security on a periodic basis.

- Will work with departments to prevent and resolve issues with security breaches, viruses and other information systems security problems.

References

- Information Technology: Acceptable Use Policy
- Cellular Phone Use Policy
- Payment Card Industry Data Securities Standards