If you have questions or comments, please contact:

Tony Campbell
Enterprise IT Security Specialist
tcampbell@rochestermn.gov
(507) 328-2848

Section 4: Physical and Environmental Security

Section 4: Physical and Environmental Security

Physical and environmental security blends information security requirements and traditional security control with the objective of preventing, deterring, and detecting, unauthorized access, damage, and interference to business premises and equipment.

Goals of Section 4: Physical and Environmental Security

- Define a multi-tier classification system for workplace security requirements.
- Ensure physical access to secure areas is restricted to authorized personnel.
- Ensure facilities and rooms housing sensitive equipment are protected from physical and environmental danger, including fire, water, smoke, and theft.
- Codify the City's commitment to sustainable computing and the minimization of power consumption.
- Create a consistent practice for media and devices disposal and destruction. Create a consistent practice for securing removable devices and media.

Physical and Environmental Security Policy Index

4.1. Physical Security Perimeter

4.1.1. The City will establish appropriate physical security perimeters around business premises.

4.1.2. An annual risk assessment of all existing business premises and information processing facilities will determine the type and strength of the security perimeter that is appropriate and prudent.

4.1.3. A risk assessment is required for all new sites under consideration prior to the finalization of building plans.

4.1.4. The IT Leadership Team will conduct risk assessments of data centers and IT systems.

4.1.5. Submission of Risk assessment results and recommendations to the Technology Steering Committee is required.

4.1.6. Department Heads, or their designees, are responsible for the implementation and maintenance of all physical security perimeter controls.

4.1.7. Areas containing Criminal Justice Information must adhere to the guidelines in section 5.9 of the CSP.

4.2. Physical Entry Controls

4.2.1. Access to all non-public City locations will be restricted to authorized persons only.

4.2.2. Department Heads, or their designees, are responsible for authorizing access credentials to employees and contractors.

4.2.3. Department Heads are required to ensure that visitor identification, access credentials, and monitoring occurs. Documentation of visitor activity is required.

4.2.4. Employees and contractors are required to display identification above the waist in all City locations at all times.

4.2.5. Visitors are required to display visitor identification in all non-public City locations.

4.2.6. Visitors to non-public areas must be escorted at all times.

4.2.7. All personnel will receive training that mandates the immediate reporting of unescorted visitors in non-public areas.

4.2.8. Areas containing Criminal Justice Information must adhere to the guidelines in section 5.9 of the CSP.

4.3. Workspace Classification

4.3.1. The City will use a three-tiered workspace classification schema consisting of secure, restricted, and public.

4.3.2. The City will publish definitions for each classification.

4.3.3. The criteria for each level will be maintained by and available by the Enterprise IT Security Specialist.

4.3.4. All locations will be associated with one of the three data classifications.

4.3.5. Classification assignment is the joint responsibility of Department Heads and the IT Leadership Team.

4.3.6. Each classification must have documented security requirements.

4.3.7. The Technology Steering Committee must authorize exceptions.

4.4. Working in Secure Areas

4.4.1. Areas classified as “secure” must be monitored by security cameras.

4.4.2. Recording of all work in areas classified as “secure” is required. Retention of the recordings for a period of 30 days is required.

4.4.3. No mobile data storage devices in areas classified as “secure” without the authorization of the Technology Steering Committee and the IT Leadership Team.

4.4.4. No Audio or video recording equipment in areas classified as “secure” without the authorization of the Technology Steering Committee and the IT Leadership Team.

4.5. Clear Desk and Clear Screen

4.5.1. When left unattended during business hours, desks should be clear of all documents classified as “high risk” or “medium risk.”

4.5.2. During non-business hours, all documents classified as “high risk” or “medium risk” should be stored in a locked office area or locked drawer.

4.5.3. Users must ensure that device displays of any type are not accessible for unauthorized viewing.

4.5.4. When left unattended during business hours, device displays should be cleared and locked to prevent viewing.

4.5.5. “High risk” and “medium risk” document printing is restricted to assigned printers and print jobs require immediate retrieval unless the print device requires user codes.

4.5.6. Scanners, copiers, and fax machines in public areas require user codes if staff have the ability to send print jobs containing non-public information to them.

4.6. Power Consumption Policy

4.6.1. The City is committed to sustainable computing and the minimization of power consumption.

4.6.2. All computing devices purchased must be Energy Star© (or equivalent) certified.

4.6.3. All end user computing devices must be configured in power save mode unless otherwise authorized by an IT manager.

4.6.4. IT Managers will assess bi-annually the best method(s) to provide clean, reliable Data Center power.

4.6.5. Protecting Data Center equipment from damage caused by power fluctuations or interruptions is required.

4.6.6. Testing Data Center power protection devices on a scheduled basis for functionality and load capacity is required and IT Managers will keep a log of all tests, service, and routine maintenance.

4.6.7. Testing Data Center generators is required according to manufacturer's instructions and IT Managers will keep a log of all tests, service, and routine maintenance to document compliance.

4.7. Data Center and Communications Facilities Environmental Safeguards

4.7.1. Smoking, eating, and drinking is not permitted in Data Center and Communications Facilities.

4.7.2. Servers and communications equipment must be located in areas free from physical danger.

4.7.3. Servers and communications equipment should be protected by uninterruptable power supplies and backup power sources. Locations with data equipment that do not have UPS and backup power sources require approval by the Technology Steering Committee based upon documentation and justification by IT Managers

4.7.4. Appropriate fire detection, suppression, and fighting equipment must be installed and/or available in all Data Center and Communications Facilities.

4.7.5. Appropriate climate control systems are required in all Data Center and Communications Facilities.

4.7.6. Emergency lighting must engage automatically during power outages at all Data Center and Communications Facilities.

4.7.7. IT Managers are responsible for managing and maintaining the Data Center and Communications Facilities climate control, fire, and power systems.

4.8. Secure Disposal Policy

4.8.1. The Enterprise IT Security Specialist will create documented disposal standards for each classification of information.

4.8.1.1. The Technology Steering Committee will review and approve the disposal standards.

4.8.2. Devices or media containing “high risk” or “medium risk” information must remain on-site for repair and/or maintenance unless the data is encrypted.

4.8.3. The standards for the highest classification must be adhered to when the device or media contains multiple types of data.

4.8.4. A chain of custody is required for the destruction of “high risk” information.

4.8.5. A Certificate of Destruction is required for third-party destruction of devices or media that contains “high risk” and “medium risk” information.

4.8.6. Disposal of media and equipment should follow all applicable state and federal environmental disposal laws and regulations.