If you have questions or comments, please contact:

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

Section 5: Communications and Operations Security

Section 5: Communications and Operations Security

Communications and Operations Security addresses information security in the context of internal and outsourced information technology operations including Data Center operations, vulnerability management, data loss protection, evidence-based logging, and vendor management.

Goals of Section 5: Communications and Operations Security

- The CIS Critical Security Controls will guide all technical control implementations
- Require documented standard operating procedures (SOPs).
- Minimize harm and maximize success associated with making changes to information systems or processes.
- Ensure timely deployment of security patches to address vulnerabilities in operating systems applications or code.
- Ensure a holistic company-wide effort to monitor critical systems and prevent, detect, and contain malicious software.
- Minimize the risk of interrupted business operations.
- Ensure a process for periodic review of system access to confirm that unauthorized access mitigation is effective.
- Extend organizational requirements to service providers.

Communications and Operations Policy Index

5.10 Software Installation

5.11 Information Transfer

5.0 Communications and Operations Policy

5.1. Standard Operating Procedures (SOPs)

5.1.1. IT managers are responsible for the publication and distribution of information systems related SOPs.

5.1.1.1. Information system custodians are responsible for developing and testing the procedures.

5.1.1.2. Information system owners are responsible for authorization and ongoing review.

5.1.2. The Enterprise IT Security Specialist is responsible for review of SOPs from an information security perspective.

5.2. Operational Change Control (Change management)

5.2.1. The IT Leadership Team is responsible for maintaining a documented change control process that provides an orderly method for requesting, approving, and informing stakeholders of, changes to production information systems and processes prior to installation and/or implementation. Changes to information systems include but are not limited to the following:

5.2.1.1. Vendor-released operating system, software application and firmware patches, updates and upgrades.

5.2.1.2. Updates and changes to internally developed software applications.

5.2.1.3. Repairing or replacing devices or individual hardware components unless the device adheres to an authorized Critical Security Controls configuration standard.

5.2.1.4. Security patch implementation is exempt from this process as long as they follow the approved patch management process.

5.2.2. The change control process must take into consideration the criticality of the system and the risk associated with the change.

5.2.3. Changes to information systems and processes considered critical to the operation of the company must be subject to pre-production testing.

5.2.4. Changes to information systems and processes considered critical to the operation of the company must have an approved rollback and/or recovery plan.

5.2.5. The Technology Steering Committee must be informed of changes to information systems and processes considered critical to the operation of the city at least 5 days in advance of the change. The business process owner must approve proposed changes. Critical systems are designated by the Technology Steering Committee based upon the results of a Business Impact Analysis.

5.2.6. Communication of changes to all impacted stakeholders is required prior to deploying the change.

5.2.7. In an emergency scenario, changes may be made immediately (business system interruption, failed server, and so on) to the production environment pending verbal approval by any member of the IT Leadership Team.

5.2.7.1. After implementing a change, written documentation of the change is required. The area's IT Manager will review the documentation.

5.3. Security Patch Management

5.3.1. Implementations of security patches are exempt from the organizational change management process as long as they follow the approved patch management process.

5.3.2. The IT Leadership Team is responsible for maintaining a documented patch management process.

5.3.3. IT Managers are responsible for the deployment of all operating system, application, and device security patches.

5.3.4. Security patches will be reviewed and deployed according to applicability of the security vulnerability and/or identified risk associated with the patch or hot-fix.

5.3.5. Testing of Security patches prior to deployment in the production environment is required.

5.3.6. Vendors who maintain company systems are required to adhere to the patch management process.

5.3.7. If a security patch installation cannot be applied to a system, notifying a member of the IT Leadership Team is required. Notification must detail the risk to the organization.

5.3.8 The Enterprise IT Security Specialist will audit and report to the Technology Steering Committee on the status of security patching across the enterprise at least quarterly.

5.4. Malicious Software (Malware/anti-virus) Protection

5.4.1. The IT Leadership Team is responsible for recommending and implementing prevention, detection, and containment controls.

5.4.2. Anti-malware software is required on all computer workstations, mobile devices, and servers to prevent, detect, and contain malicious software.

5.4.3. Any system found to be out-of-date with vendor-supplied definitions and/or detection engines requires remediation, failing that disconnecting the system from the network until the system is up to date is required.

5.4.4 Reporting all malware-related incidents to the IT Leadership Team is required.

5.5. Data Replication

5.5.1. The IT Leadership Team is responsible for design and oversight of the enterprise replication and backup strategy. Factors for consideration include but are not limited to business impact, cost, regulatory requirements, and appropriate Recovery Time Objectives and Recovery Point Objectives.

5.5.2. Data contained on replicated or backup media requires appropriate control based on its classification.

5.5.3. IT Managers are responsible for the implementation, maintenance, and ongoing monitoring of the replication and backup/restoration strategy.

5.5.4. Documentation of the process is required.

5.5.5. Testing the procedures on a scheduled basis is required.

5.5.6. Backup media no longer in rotation requires disposal in accordance with the organization's destruction standard.

5.5.7. The IT Leadership Team will provide the Technology Steering Committee with an annual update on the status of data replication.

5.6. Email and Email Systems Security

5.6.1. The Enterprise IT Security Specialist is responsible for assessing the risk associated with email and email systems. Risk assessments should occur at least annually.

5.6.2. The Enterprise IT Security Specialist will recommend email security standards for approval by the Technology Steering Committee.

5.6.3. External transmission of data classified as "high risk" or "medium risk" requires encryption.

5.6.4. Remote access to company email must conform to the corporate remote access standards.

5.6.5. No personnel may access personal web-based email systems or unauthorized external storage from the City's networks or on City-owned devices.

5.6.6. IT managers are responsible for implementing and maintaining appropriate controls.

5.6.7. Human Resources and the Enterprise IT Security Specialist are jointly responsible for providing email security awareness training to users.

5.7. Security Log Management

5.7.1. Devices systems, and applications implemented by the company must support the ability to log activities.

5.7.1.1. The IT Leadership Team must approve any exceptions.

5.7.2. Access to logs must be restricted to individuals with a need-to-know.

5.7.3. The Enterprise IT Security Specialist will recommend standards, procedures, and guidelines for managing log files for approval by the Technology Steering Committee.

5.8. Service Provider Management

5.8.1. A service provider is a vendor, contractor, business partner, or affiliate, who stores, processes, transmits, or accesses company information or company information systems.

5.8.2 The Business Process Owner and the Enterprise IT Security Specialist will be responsible for conducting applicable risk assessments pertaining to service providers. Results must be reported to the Technology Steering Committee.

5.8.3 Due diligence research is required on all service providers. Depending upon risk assessment results, due diligence research may include but is not limited to financial soundness review, internal Information Security Policy and control environment review, and review of any industry standard audit and/or testing of information security-related controls.

5.8.4 Service provider system safeguards must be commensurate with the classification of data and the level of inherent risk.

5.8.5 Contracts and/or agreements with service providers must specifically require them to protect the Confidentiality, Integrity, and Availability of all company, customer, and proprietary information that is under their control.

5.8.6 Contracts and/or agreements must include the following:

5.8.6.1 Notification requirements for suspected or actual compromise or system breach, preferably within 72 hours.

5.8.6.2 A signed statement showing that the service provider acknowledges the obligation to comply with all applicable state and federal regulations.

5.8.6.3 A Provision for periodic security reviews/audits of the service provider environment.

5.8.6.4 A Provision requiring that service providers disclose their use of contractors, and third party data centers or services, and ensure that the same adhere to the identical contract terms agreed to by the provider and the City.

5.8.6.5. As applicable, a clause related to the proper destruction of records containing customer or proprietary information when no longer in use or if the relationship terminates.

5.8.6.6 To the extent possible and practical, contractual performance will be monitored and/or verified.

5.8.7 The business process owner, the Enterprise IT Security Specialist, and the City Clerk are jointly responsible for annual risk assessments of existing service providers.

5.9. Mobile device and Media Security

5.9.1. All company-owned and employee-owned mobile devices and media that store or have the potential to store City information classified as “high risk” or “medium risk” require encryption.

5.9.2. Whenever feasible, an anti-theft technology solution that enables remote locating, remote locking, and remote delete/wipe functionality is required.

5.9.3 Mobile devices must utilize screen locks with (in order of preference) biometric, password, or passcode required to unlock.

5.9.4. Loss or theft of mobile devices or media requires immediate reporting to the IT Leadership Team.

5.10 Software installation

5.10.1. All software installed on company-owned systems requires authorization by the IT Leadership Team with the Technology Steering Committee serving as the final level of appeal.

5.10.2. All authorized software must be identified in an authorized software inventory database.

5.11 information transfer

5.11.1 All data classified “high risk” requires encryption both in transit and at rest.

5.11.2 All data classified “medium risk” requires encryption at rest.

5.11.3 All data classified “medium risk” requires encryption in transit outside of internal networks.