If you have questions or comments, please contact:

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

Section 7: INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE

Information Systems Acquisition, Development, and Maintenance focuses on (1) the lifecycle of information systems and components and (2) internal software development. The purpose of this section is to require secure practices from initiation through disposal. Our Primary goals are:

- Ensure a structured and standardized process for all phases of system development/acquisition efforts that includes security considerations, requirements, and testing.

- Define the requirements for the implementation and maintenance of commercial and open source software.
- Define code and application security requirements.
- Assign responsibility for key management and cryptographic standards.

Information Systems acquisition, development, and maintenance index

7.1. System Development Lifecycle (SDLC)

7.2. System Implementation and Maintenance

7.3. Application Development

7.4. Key Management

7.1. System Development Lifecycle (SDLC)

7.1.1. The Technology Steering Committee is responsible for adopting, and implementing an SDLC process and workflow.

7.1.2. At each phase, security requirements require evaluation and, as appropriate, testing of security controls.

7.1.3. The system owner in conjunction with the IT Leadership Team is responsible for defining system security requirements.

7.1.4. The system owner in conjunction with the IT Leadership Team, is responsible for authorizing production systems prior to implementation.

7.1.5. If necessary, independent experts may evaluate the project or any component thereof.

7.2. System Implementation and Maintenance

7.2.1. Operating systems and applications (collectively referred to as “system”) implementation and updates must follow the company change management process.

7.2.2. No one may authorize or deploy applications in alpha, beta or a prerelease state on the organization’s production systems.

7.2.3. It is the responsibility of the application owner to conduct functional testing prior to deployment in the production environment.

7.2.4. It is the responsibility of IT management in coordination with the application owner, to conduct security testing prior to deployment in the production environment.

7.2.4. IT Management is responsible to budget for and maintain a test environment that is representative of the production environment.

7.2.5. Without exception, data classified as “high risk” is not deployable to a test environment without first anonymizing.

7.2.6 Without exception, data will be securely removed (degaussed) or rendered unreadable from systems prior to disposal.

7.3.7 The IT Leadership Team will adopt and implement a secure disposal process.

7.3.8 The Enterprise IT Security Specialist will review and approve secure disposal standards.

7.3. Application Development

7.3.1. IT leadership will determine the impacted data’s classification level, subject to confirmation by the City Clerk, prior to any application development.

The developed application requires an application penetration test or proof that the current version of the deployed application has passed application security vulnerability testing within the past 24 months if the application involves data classified as anything other than Low Risk.

7.3.2. Security requirements for application development require documentation.

7.3.3. Code development must follow industry best practices.

7.3.4. Developers must have adequate training, resources, and time.

7.3.5. At the discretion of the system owner and with the approval of the IT Leadership Team, third parties may be engaged to design, develop, and test internal applications.

7.3.6. All code developed or customized must follow the change control/review process before development is started.

7.4. Key Management

7.4.1. The IT Leadership Team is responsible for key management including but not limited to algorithm decisions, key length, and key security and resiliency.

7.4.2. The Enterprise IT Security Specialist will review and recommend action to the Technology Steering Committee for approval of cryptographic standards.

7.4.3. Without exception, encryption is required whenever transmitting “High” or “Medium” risk information externally. This includes email and file transfer. The encryption mechanism must be NIST approved.

7.4.4. Without exception, encryption is required on all removable media that stores or has the potential to store “High” or “Medium” risk information. The encryption mechanism must be NIST approved.

7.4.5. Data at rest requires encryption regardless of media when state and/or federal regulation or contractual agreement mandate encryption.

7.4.6. At all times, passwords and PINs must be stored and transmitted as cipher text.