If you have questions or comments, please contact:

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

# Section 1: GOVERNANCE AND RISK MANAGEMENT

Governance is the set of responsibilities and practices exercised by management with the goal of ensuring that the City; provides strategic direction, meets its business objectives, manages risk appropriately, verifies responsible use of its resources, and aligns with applicable laws and regulations. The principal objective of our City's risk management process is to provide those in leadership and data steward roles with the information required to make well-informed decisions regarding the CIA of our data and services. Our primary goals are:

- To demonstrate the governing boards' commitment to implementing and maintaining an Information Security Program and supporting policies.

- To ensure that management is actively engaged in the operation and effectiveness of the Information Security Policy and Program.
- To provide the support and oversight required to maintain an effective policy and program.
- Defining organizational roles and responsibilities, and providing the framework for effective risk management and continuous assessment.

## *Governance and Risk Management Policy Index*



## 1.1 Information Security Policy

1.1.1. The City is required to have a written Information Security Policy and supporting documents.

1.1.2. The City Council and governing boards are responsible for establishing the mandate and general objectives of the aggregate Information Security Policy.

1.1.3. Information security policies must consider organizational objectives.

1.1.4. Information security policies must comply with relevant statutory, regulatory, and contractual requirements (e.g. MN Data Practices Act, PCI, CJIS, **CIPA**, and HIPAA).

1.1.5. Information security policies should be communicated to all relevant parties both within and external to the City.

1.1.6. As applicable, the City will develop standards, guidelines and procedures to support the implementation of Information Security Policy objectives and requirements.

1.1.7. Our Information Security Policy contains non-public information. The policy and supporting documents may not be distributed outside of the City. Pursuant to the Minnesota Government Data Practices Act provision addressing security information (Minn. Stat. section 13.37) and Commissioner of Administration Opinion #02 014 issued April 5, 2002, the City of Rochester's information regarding the design, operation, maintenance, control, or access to any and all of its IT security strategies and functions has been declared to be not public information that cannot be disclosed to the public in order to protect and maintain the public's health, safety, and welfare.

1.1.8. All documentation is subject to standard document retention policies per the City Clerk's office policies.

## 1.2 Information Security Policy Authorization and Oversight

1.2.1. The City Council authorizes the Information Security Policy.

1.2.2. The Information Security Policy requires review at least annually or by request from department heads or the IT leadership Team.

1.2.2.1. The Enterprise IT security Specialist will manage the review process.

1.2.3. Changes to the policy require approval by department heads.

1.2.4. The **IT Leadership Team** will present, at least annually, a report to the Technology Steering Committee. The report should provide them the information necessary to measure the Citys' adherence to the Information Security Policy objectives and the maturity of the Information Security Program as well as updates on current, or emerging, risks and assessments.

1.2.5. When in-house knowledge is not sufficient to review or audit aspects of the Information Security Policy, or if circumstances dictate independence, the city will engage third-party professionals.

## 1.3 Roles and responsibilities

1.3.1. The IT Leadership Team membership includes the Enterprise IT Security Specialist and the IT Manager for the City, Rochester Public Utilities (RPU), and Rochester Public Library (RPL). The Technology Steering Committee may appoint additional parties to the IT Leadership Team.

1.3.2. The IT Leadership Team is responsible to work with department heads in managing the Information Security Program, assuring compliance with applicable regulations and contractual obligations.

1.3.2.1. The IT leadership Team will work with the business owner to align security requirements with business objectives.

1.3.2.2. When agreement cannot be reached between the business owner, IT Leadership Team, and the Technology Steering Committee on security requirements, the City Administrator shall serve as the final point of escalation.

## 1.4 Segregation of duties

1.4.1. The city Director of Finance and IT and the Chief Financial Officer/CIO of RPU are responsible to ensure that critical tasks are appropriately segregated.

1.4.2. The Enterprise IT Security Specialist is responsible for annual review/audit of segregation of critical tasks.

## 1.5 Information Security Risk Management Oversight

1.5.1. The Technology Steering Committee in consultation with department heads and the IT Leadership Team is responsible for determining the overall risk appetite and risk tolerance levels.

1.5.2. The Technology Steering Committee and the City Administrator will communicate the above to decision makers throughout the City.

## 1.6 Information Security Risk Assessment

1.6.1. The City has adopted the CIS Critical Security Controls and the NIST Cybersecurity Framework as a guide for its information security risk assessment methodology to ensure consistent, repeatable, and comparable results.

1.6.2. Information security risk assessments must have a clearly defined and limited scope. Assessments with a broad scope become difficult and unwieldy in both their execution and the documentation of the results.

1.6.3. The Technology Steering Committee and the Enterprise IT Security Specialist will develop an information security risk assessment schedule based upon the information systems criticality and information classification level.

1.6.4. In addition to scheduled assessments, information security risk assessments are required prior to the implementation of changes in technology, process, or third-party agreement involving regulated, confidential or private information.

1.6.5. The Enterprise IT Security Specialist is responsible for security assessments of networks and systems at least annually.

1.6.5.1 The City Clerk is responsible for security assessments of data and physical records at least annually.

1.6.6. The IT Leadership Team will review risk assessment results and make recommendations to the Technology Steering Committee.

## 1.7 Information Security Risk Response

1.7.1. Presentation of the initial results of all risk assessments to the Technology Steering Committee must occur within 45 days of completion.

1.7.2. Department heads may accept low-level risks.

1.7.3. High risks require a response within 45 days. Response is the joint responsibility of the IT Leadership Team and the Technology Steering Committee.

1.7.3.1. Risk reduction recommendations can include risk acceptance, risk mitigation, risk transfer, risk avoidance, or a combination thereof.

1.7.3.2. Risk evaluations, recommendations and decisions will be documented and include an appropriate level of detail of risks, assumptions, mitigations and persons approving of denying a request.

1.7.4. The City Administrator may accept High risks.

1.7.5. Notification of the acceptance of Critical risk to the IT Leadership Team, governing boards and the Technology Steering Committee is required.

## 1.8 Policy Exceptions

1.8.1 Where compliance is not technically feasible, jeopardizes employee safety, or causes severe adverse impact to the business, an exception may apply. Exception requests require a written submission, including justification, to the IT Leadership Team (Enterprise IT Security Specialist and IT Managers

for the City, Rochester Public Utilities, and Rochester Public Library). Granting the exception request is at the discretion of the IT Leadership Team and the Technology Steering Committee, with the City Administrator serving as the final level of appeal.

1.8.1.2 Any member of the IT Leadership Team may unilaterally grant an exception in the event of an emergency (defined as a serious, unexpected, and often dangerous situation requiring immediate action). The individual granting the emergency exception must document the exception and notify the other members of the IT Leadership Team of the emergency exception within 24 hours. The IT Leadership Team must review and act upon any emergency exception within 30 days.

1.8.1.3 The IT Leadership Team will provide the Technology Steering Committee with a summary report on exceptions at least quarterly. The Governance section of our online library will house documentation of all exceptions following standard document retention policy.

**PCI or PCI\DSS:** Payment Card Industry Data Security Standard

**CIPA**: Children's Internet Protection Act

**CJIS**: Criminal Justice Information Services

**IT Leadership Team**: Consists of the Enterprise IT Security Specialist and the IT Managers for the City, Rochester Public Library, and Rochester Public Utilities