

If you have questions or comments, please contact:

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

Human Resources Security

Section 2: Human Resources Security

Information security is primarily a people-driven process; it is imperative that information owners, custodians, and users embrace the policy. Embedding Personnel-related security controls in each stage of the employee lifecycle: recruitment, onboarding, user provisioning, orientation, career development, and termination are imperative.

Goals of Section 2: Human Resources Security

- Ensure the protection of City and candidate resources during the recruitment process.
- Set the parameters for workforce background checks.
- Require an enterprise-wide user provisioning process.
- Define electronic monitoring activities, privacy rights, and employee consent.
- Ensure employees are aware of their responsibilities when using, or supporting, city technology.
- Ensure the application of disciplinary action, up to and including termination is consistent and fair according to the standard and attendant policies, procedures, and guidelines.
- With input from the IT staff, ensure all full-time employees, contractors, interns, and designated third parties receive training appropriate to their position throughout their tenure.

Human Resources Security Policy Index

2.1. [Recruitment](#)

2.2. [Personnel Screening](#)

2.3. [User Provisioning](#)

2.4. [Electronic Monitoring](#)

2.5. [Employee Termination](#)

2.6. [Employee Agreements](#)

2.7. [Information Security Training](#)

2.1. Recruitment

2.1.1. Any information classified as “medium risk” or “high risk” must not be included in job postings or job descriptions.

2.1.2. Candidates entering office areas (other than reception or other public areas) should be escorted at all times. Candidates accessing secure areas must be escorted at all times.

2.1.2. All non-public information submitted by candidates requires classification as “medium risk” and must remain in accordance with City medium risk data handling standards.

2.1.4 Under no circumstances, will the City request that candidates provide a password to social media, blog, web, or personal email accounts.

2.1.5. Human Resources and Department Heads will be jointly responsible for the implementation and enforcement of this policy.

2.2. Personnel Screening

2.2.1. As a condition of employment, all full-time and part-time regular employees are subject to background screening. Further, any independent contractor doing business with the City may also be subject to a background screening process.

2.2.2. Background screening for employee candidates is a pre-hire requirement.

2.2.2. Background screening must comply with local, state, and federal law and regulations.

2.2.4. If the person will have access to “high risk” or “medium risk” information, additional screening may be required at the discretion of the information owner. This includes new personnel as well as current employees moving into such a position.

2.2.5. Background screening is the responsibility of Human Resources except where the candidate is applying to the police department or applies as a seasonal employee. The Rochester Police Department conducts all background screening for sworn officer candidates, and Department Heads, or their designees, will conduct background screening for their seasonal employees.

2.2.6. If temporary or contract staff are provided by an agency or third party, the contract must clearly specify the agency or third-party responsibility for conducting background checks in accordance with this policy. The Human Resources department must have access to the results of the background check.

2.3. User Provisioning

2.3.1. There will be a defined and documented user provisioning process for granting and revoking access to City resources that includes but is not limited to account creation, account management including assignment of access rights and permissions, periodic review of access rights and permissions, and account termination.

2.3.2. The Human Resources Department, other individual Departments and the Enterprise IT Security Specialist are jointly responsible for the User Provisioning process.

2.4. Electronic Monitoring

2.4.1. The City reserves the right to monitor electronic activity on City-owned information systems including but not limited to voice, email, text and messaging communications sent, received, or stored, computer and network activity, and Internet activity including sites visited and actions taken.

2.4.2. Employees, as part of the hiring process, must be notified that their activities on city technology may be monitored.

2.4.3. Whenever technically feasible, login banners and warning messages will remind users of their responsibilities when using, or supporting, city technology and that their activity may be monitored

2.4.4. Human Resources and the Enterprise IT Security Specialist are jointly responsible for developing and managing electronic monitoring and employee notification.

2.5. Employee Termination

2.5.1. Upon the termination of the relationship between the City and any employee, all access to facilities and information resources shall cease.

2.5.2. In the case of an involuntary termination, all physical and technical access will be disabled pre-notification.

2.5.2. In the case of employment retirements or other voluntary separations,, Human Resources is responsible for determining the schedule for disabling access.

2.5.4. Termination procedures are to be included in the User Provisioning Process.

2.5.5. Human Resources and the Enterprise IT Security Specialist are jointly responsible for the User Provisioning process.

2.6. Employee Agreements

2.6.1. All employees should receive training prior to being provided any City information classified as high or medium risk.

2.6.2. All employees must sign an acceptable use policy prior to being granted access to any City information or systems.

2.6.3. The Enterprise IT Security Specialist in collaboration with department heads is responsible for developing, maintaining, and updating the confidentiality agreement.

2.6.4. Human Resources and the Enterprise IT Security Specialist are jointly responsible for developing, maintaining, and updating the acceptable use policy.

2.6.5. Human Resources is responsible for distributing the policy and managing the acknowledgment process.

2.7. Information Security Training (Security Awareness)

2.7.1. The Human Resources department is responsible for information security training during the employee orientation phase. The training must include compliance requirements and City policies.

2.7.2. Subsequent training will occur at the departmental level. Training on the use of departmental systems appropriate to the user's specific duties will ensure the Confidentiality, Integrity, and Availability of information.

2.7.2. Annual information security training is the responsibility of the Technology department. Staff participation is required and Human Resources will maintain participation records. At a minimum, training will include the following topics: current information security-related threats and risks, security policy updates, and reporting of security incidents. Content of the training is the responsibility of the Enterprise IT Security Specialist. The Human Resources department will periodically review the training content. Delivery of the training is the joint responsibility of the IT Department and the Enterprise IT Security Specialist.