RAMSEY COUNTY
Human Resources

# Job Class Title: IS Chief Information Security Officer (Unclassified)

**BASIC FUNCTION:**
To manage the development and implementation of a county-wide information security program to ensure that information assets are adequately protected; to identify, evaluate, and report on information security risks in a manner that meets compliance and regulatory requirements; to work with executive management to determine acceptable levels of risk for the county; to work proactively with departments to implement practices that meet defined policies and standards for information security; and to perform related duties as assigned. This role will also contribute to achieving the overall county information technology (IT) vision as a part of the IS Senior Leadership team.

**EXAMPLES OF WORK PERFORMED:**
1. Promote a diverse, culturally competent and respectful workplace.
2. Provide information security leadership and direction through the continued development, implementation, and maintenance of the enterprise information security program.
3. Advocate for and protect enterprise security by serving as the key information security advisor to the organization and act as the official information security representative to internal customers, external partners, audit and regulatory organizations.
4. Build a comprehensive enterprise security strategy which includes implementing, directing, and overseeing the governance, assessment, consulting, monitoring and reporting functions.
5. Develop, implement, update and enforce county-wide information security policy, procedures, guidelines, and standards to ensure county-wide compliance with federal and Minnesota statutory and regulatory requirements for information security including the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Criminal Justice Information Services (CJIS) requirements and other applicable requirements.
6. Consult with management on information security matters, such as the effect of state and federal laws, industry related regulations, and industry best practices on security related initiatives, projects, business operations, and department specific policy.
7. Monitor information security trends internal and external to Ramsey County, understand potential threats, vulnerabilities and control techniques and provide consultation to executive management and departments about information security issues and risks affecting the organization and advise them on the appropriate actions to be taken.
8. Maintain relationships with local, state and federal law enforcement and other related government agencies.
9. Establish and maintain effective relationships and work collaboratively across departments to facilitate IT risk analysis and risk management processes, identify acceptable levels of risk, initiate business practice changes and establish roles and responsibilities to ensure data is protected.
10. Ensure the security of the remote and mobile computing environment.
11. Provide strategic and tactical security guidance for all IT projects, including the evaluation and recommendation of technical controls.
12. Manage security incidents and events to protect IT assets and data. Act as a central point of contact for all data security compromising incidents, develop incident handling procedures, and report incidents as required by law.
13. Perform supervisory tasks such as completing performance evaluations, recognizing and addressing performance problems, hiring staff, mentoring and coaching.
14. Create and facilitate the information security risk assessment process, including reporting to executive management and oversight of remediation efforts to address findings.
15. Create and manage a county-wide information security and risk management awareness training program.
16. Develop and manage effective recovery plans that ensure data privacy and information integrity in response to business need and compliance requirements in the event of a disaster. Provide leadership

with updates of the development, documentation and maintenance of the county-wide disaster recovery plans.
17. Monitor and report on county information, security activities and compliance.

*(The work assigned to a position in this classification may not include all possible tasks in this description and does not limit the assignment of any additional tasks in this classification. Regular attendance according to the position's management approved work schedule is required.)*

**ESSENTIAL FUNCTIONS:** 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17.

**SUPERVISOR/MANAGERIAL RESPONSIBILITY:**
Manages the work of 4+ (FTEs) including information security services staff members and project teams. Oversees performance of contractors and consultants, as well as 3rd party 24/7 operation service providers.

**INTERNAL/EXTERNAL RELATIONSHIPS:**
Daily contact with supervisors, managers, and directors of county departments and outside vendors to define problems and needs, develop and present useful solutions, advice on information security aspects of information security of projects, establish priorities, resolve conflicts and coordinate implementation of information security solutions. Daily to weekly contact with executive level management to determine acceptable levels of risk for the county, provide consultation and advise them on the appropriate actions to be taken. Daily to weekly contact with the State of Minnesota regarding information security coordination and network monitoring. Weekly contact with information security professionals in other jurisdictions to establish and maintain relationships and to confer and consult. Weekly to monthly contact with governmental and private agencies regarding security requirements. Monthly contact with state and internal auditors as the point of county coordination regarding security and risk issues. Occasional contact with elected representatives to discuss issues, provide consultation, gather information for further assessment or resolve issues related to the county's information security program.

**IMPACT ON SERVICES/OPERATIONS:**
Impacts the confidentiality, integrity and availability of all county data and information systems. Proper performance ensures that the county's data and information systems will be protected and in compliance with applicable state and federal laws, and standards for information security. Improper performance could result in ineffective programs, security risks, data breach, loss of data, excessive downtime or delays in response to disaster and potential liability for the county. Poor performance can also result in an information system that is inefficient or fails to meet the needs of users; ineffective recommendations of software, hardware, systems or services to use departments; and inadequate provision of training services for users.

**WORK ENVIRONMENT:**
Work is performed primarily in a standard office environment, work involves operation of personal computer equipment up to six hours a day. Travel to various worksites is also required to attend meetings. May require extended hours and work from home. Require constant multi-tasking, frequent interruptions, and numerous meetings with county staff and management. Consult with and serve on county-wide committees and initiatives representing county management.

**KNOWLEDGE, SKILLS AND ABILITIES REQUIRED:**
- Knowledge of the principles and practices of information systems and information security.
- Knowledge of technological trends and developments in the area of information security and risk management.
- Knowledge of common information security management frameworks, such as ITIL and COBIT.
- Knowledge of organizational and management principles.
- Knowledge of the complexities and interdependencies of the county's functions and departments.

- Knowledge of federal and state information security laws and regulations.
- Skill in critical thinking, with strong problem-solving skills. Poise and ability to act calmly and competently in high-pressure, high stress situations.
- Ability to communicate security and risk-related concepts to technical and non-technical audiences.
- Ability to define and analyze issues and problems, evaluate alternatives, and develop sound independent conclusions and recommendations in accordance with laws, regulations, rules and policies.
- Ability to develop and maintain effective working relationships with vendors, end users, supervisors, managers, directors and elected officials.
- Ability to foster inter-agency and inter-governmental cooperation for the implementation, enforcement, and compliance with information security policy.
- Ability to represent the information systems perspectives to other members of various county-wide or cross-departmental groups.
- Ability to effectively communicate complex concepts in spoken and written communications.
- Ability to work effectively in a changing environment with minimal to no supervision to meet deadlines.
- Ability to identify barriers and propose solutions which meet departments' information security needs.
- Ability to lead and motivate cross-functional, interdisciplinary teams to achieve tactical and strategic goals.
- Ability to facilitate compromise between agencies and individuals, sometimes with competing interests and needs.

**MINIMUM QUALIFICATIONS:**
Education: Bachelor's Degree in management information systems, computer science or a related field.

Experience: Five years of progressively responsible information technology experience in the areas of security and risk management, including at least two years in a leadership role.

Substitution: None.

Certifications/Licensure: None.

Preferred Experience: Professional certification, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified information System Auditor (CISA) or other information security credentials.

Revisions: 9-2-22; 1-27-16; 7-28-11; 12-14-10.