ST CLOUD STATE UNIVERSITY
VACANCY POSTING

This posting is effective **January 14, 2025** and expires **January 21, 2025.**

Eligible employees* may indicate interest in this vacancy by submitting their interest in writing to the Human Resources office during its regular business hours on or before **January 21, 2025.**

JOB NO. 0125-22	**WORK AREA** Campus
CLASS & EMPLOYMENT CONDITION Systems Supervisor Full time, Unlimited	**NORMAL HOURS OF WORK** Monday through Friday 8:00am-4:30pm

GENERAL DESCRIPTION OF JOB

This position exists to provide vision and leadership for developing and supporting IT security initiatives throughout the organization. The Systems Supervisor (Chief Information Security Officer and architecture, or CISO) directs the planning and implementation of enterprise IT systems, business operation and facility defenses against IT security breaches and vulnerability issues. This individual is also responsible for auditing existing systems, while directing the administration of security policies, activities and standards. This position is the primary contact for all IT security issues on campus. Reduce on-prem footprint and surface attach, reduce # OS instances to secure/maintain, leverage SaaS alternatives to shift to globally available, modern, and secure platforms. Continue to automate infrastructure change management and invest in our team by researching and learning more about next generation services, align infrastructure to enable the business to achieve a more seamless experience while reducing business, technical, and financial risk. Innovative and modernized approach to advance IT (IDM, platforms, knowledge, skills, tools, OS, audit and compliance, incident response and education and awareness training. The Systems Supervisor (CISO) oversees, implements and monitors the security and business continuity requirements levied by department and institution procedures and policies, Minnesota State policies and procedures, as well as local, state and federal laws, regulations, guidelines and business and industry standards

Minimum Qualifications

- Bachelor's degree from an accredited college or university in computer science, information technology, engineering, business administration or related field or an equivalent combination of education and data security experience.
- CISSP certification: To be considered for this position you must have current CISSP certification or obtain CISSP certification within your probationary period.
- Five years of related IT experience in data security including a combination of the following:
    - 3 years' experience in database design and analysis, secure networking, application development, or system administration within a complex enterprise environment
    - 3 years' experience leading and managing large-scale technology projects and ensuring plans are detailing deliverables and resources needs and
    - 3 years' experience supervising or leading data security or architecture personnel.
- Ability to create a successful team by engaging the right people, drawing out and fully leveraging individual strengths of those on the team. Strong ability to set clearly defined, attainable expectations to team members and provide mentoring and coaching.
- Advanced problem-solving abilities sufficient to analyze situations and make decisions based upon research, understanding impact of risks, and negotiation with other individuals and groups.
- Considerable knowledge of business theory, business processes, management, budgeting and business office operations.
- Experience in planning, organizing and developing IT security and facility security system technologies including security standards.
- Substantial exposure to data processing, hardware platforms, enterprise software applications,

custom application development, data integration, outsourced systems and cloud platforms.

- Demonstrated experience with implementing information security regulations including PCI, HIPAA, FERPA.
- Experience implementing current robust security controls and processes for infrastructure, applications, data, and identity/access management across local and cloud environments. This includes global technology security issues and threats.
- Experience in maintaining knowledge of department and institution procedures and policies, standards developments, Minnesota State policies and procedures, as well as local, state and federal laws, regulations, guidelines and business and industry standards.
- Strong written and verbal communication skills sufficient to write, prepare, and edit materials such as memos, procedures, reports, presentations etc. Communication skills sufficient to participate in discussions and communicate technical ideas and procedures to technical and non-technical staff and senior leadership.
- Customer services skills sufficient to actively listen to and understand customer needs and provide accurate information and appropriate alternatives in a timely, thorough, courteous, respectful and professional manner in person, over the phone and in writing.

Preferred Qualifications

- Professional experience in higher education.
- Knowledge and implementation of enterprise risk management (ERM) frameworks.
- Cloud knowledge and implementation specifically PaaS and SaaS.
- Data security contract terms and condition expertise.
- Multiple current and relevant industry certification in security (CISSP, CISM, CISA, CRISC, and CHPS)
- Knowledge of information security standards (e.g., ISO 27001/27002, etc.) rules, regulations related to information security and data confidentiality (e.g., FERPA, HIPAA, PCI, MGDPA, etc.)
- Additional data security professional certifications.

*__To be eligible to express an interest bid, an employee must be in the same class/class option as this vacancy.__