POSITION ANNOUNCEMENT

Information Security Officer
The University of Nebraska is accepting applications for an Information Security Officer (ISO) for Computing Services Network. The ISO acts in a supporting role to the Chief Information Officer (CIO) to help plan and facilitate the information security goals and objectives for the University of Nebraska.

Job Description Summary:
Working with the CIO, Central Administration legal team, and the campus security offices and technical teams, the ISO will be the primary position to communicate and enforce IT security compliance based on appropriate federal, state and University mandates, and lead in the development of IT security policy, procedures and security risk assessment for the University. The ISO will work to create an information security architecture to protect and secure the data and systems of the University of Nebraska. As the University develops more complex, distributed and integrated information systems, new methods and underlying security controls and structure will require review, recommendation and improvements. This position will also work with the campuses and Central Administration staff to develop a recognized protocol for security event and incident management for University systems and data.

Duties include:

Security Administration:
Develop and monitor practices to ensure that the University’s administrative and academic information is secure from unauthorized access, protected from inappropriate alteration, physically secure, and available to authorized users in a timely fashion. Manage development and implementation of enterprise wide security policy, standards, and guidelines. Lead in the development of specific components of an information security architecture including:

- Create a risk assessment of all information systems and data necessary to evaluate the appropriate and most cost effective protection measures;
- Develop and communicate well defined policies and procedures for security and information systems use to all personnel;
- Develop an ongoing compliance and measurement process for information security standards; coordinate the establishment of well-defined barriers and monitoring tools between trusted and untrusted network environments; and assist in implementing development standards that ensure appropriate design of controls and security into new applications and enhancements to critical application.
- Develop a recognized protocol for security event and incident management.

IT Security Planning:
Identify protection goals and objectives consistent with University mission and strategic plan. Evaluate and make recommendations for long-range security planning in response to future systems, new technology, and new organizational changes. Identify key security program elements.

Identity Management:
Manage the Identity Management (IDM) program, including managing the strategy, structure, oversight, and ensuring compliance with operational process and procedures. This individual will lead the IDM teams and be responsible for operational processes and maintaining compliance with various requirements. This person is responsible for governing the identity lifecycle processes around
roles/rules, monitor access control processes to ensure their effectiveness and efficiency and compliance with standards and control objectives in order to adopt identity governance processes.

Security Awareness:
Training and dissemination of security policies and practices as well as developing strategies and plans to provide for timely business resumption in the event of serious disruptions.

Qualified Candidate Requirements:

- Bachelor’s degree in computer science, MIS, business administration or related field.
- An IT professional with 7-10 years of experience with demonstrated experience in managing systems projects across a decentralized organization;
- IT security management experience (3-5 years) with competent knowledge of security technologies, standards, and networking architectures;
- Experience in creating a comprehensive security compliance plan based on national or international security standards is preferred;
- Ability to identify, analyze and evaluate technology risk as well as measure the risk quantitatively and qualitatively;
- Experience with the federation of identity management across the organization. Knowledge of “In-Common” and open SSO is preferred;
- Proven experience working effectively in a team setting, collaborating with a diverse group of people, demonstrating leadership skills to manage the complexity across a variety of IT operational areas;
- Experience managing both small and large groups on a day-to-day basis as well as for specific project purposes; proven experience handling multiple projects with various deadline requirements;
- Project management skills and abilities that involved in-depth analyses resulting in detailed written reports including recommended courses of action;
- Successful candidates will exhibit the following personality traits: Highly ethical, motivated, a leader who seeks best outcomes by involving or through others, identifies what motivates others and influences appropriately, etc.; Must think conceptually, should be optimistic, positive, resilient, insightful, performance driven, an effective communicator, a decision maker, problem solver, and consensus builder.
- Experience in higher education is preferred.
- Certified Information Security Professional (CISSP) is desired.

Equivalent combination of education, experience, and training that provides the required knowledge, skills, and abilities may be considered.

Apply on line at [https://careers.nebraska.edu](https://careers.nebraska.edu) and attach a letter of application providing details about professional experience and talents applicable to this position; a current resume; and the names, addresses and telephone numbers of three professional references.

More information about CSN is available at [http://csn.nebraska.edu](http://csn.nebraska.edu)

Application review begins March 1, 2013 and continues until position is filled.

The University of Nebraska is an Affirmative Action/Equal Opportunity Institution and participates in E-Verify.