

Position Description for Contract Professional Appointments

Montana State University

<input type="checkbox"/>	Vacant Position-No Change
<input type="checkbox"/>	Vacant Position-Revised
<input type="checkbox"/>	New Position
<input checked="" type="checkbox"/>	Revised Position Description for Incumbent
Position Number: 4C0186_____	
Department: Information Technology Center	

1. General Information

01/01/2009	Chief Security Officer
_____	_____
Date	Position Title
Adam Edelman	_____
_____	_____
Name of Incumbent	Employee Signature

2. Required Signatures

_____	_____	_____
Immediate Supervisor	Printed Name	Date
_____	_____	_____
Department Head	Printed Name	Date
_____	_____	_____
Dean/Director/VP	Printed Name	Date

3. General Statement Describing Expectations of the Position.

(In one or two sentences, summarize the purpose of the position)

The Chief Security Officer reports directly to the CIO, providing high level strategic direction, planning, analysis and auditing of security technology, policy, and support functions for the four-campus enterprise information technology systems. This position is responsible for leading the enterprise wide security efforts including the development and implementation of policies and procedures, incident response, educational

outreach, technical consultation, and ongoing operations to ensure the confidentiality, integrity, and availability of the University's computing resources. The CSO will be responsible for the development and implementation of a University-wide security awareness training program.

4. Duties and Responsibilities.

(List essential functions (primary duties) of the position.)

Manage security policy, standards, and procedures

To ensure best practices are instituted throughout the four-campus enterprise, the CSO will:

- a. Determine need for security policies, procedures, and standards
- b. Write the policies, procedures, and standards
- c. Guide the review, vetting, and approval process
- d. Publish and review subsequent comment and input
- e. Maintain the policies and assists in promoting awareness and compliance

Lead Information Security Efforts

To focus team activities on security policy, procedure, and compliance issues, and to seek synergies among various security service providers, the CSO will:

- a. Lead the activities of the 4-campus Information Security Committee and distributed security practitioners
- b. Develop a shared understanding of security strategies, policies, procedures
- c. Determine methods to test for compliance, and to handle security breach incidents
- d. Task security managers and security associates with reviewing and reporting on internal controls and security procedures in their respective areas
- e. Seek quality improvements in these procedures both to improve efficiency and to mitigate risk across the security fabric of the enterprise
- f. Manage the Enterprise Security Group staff, directing tasks, setting goals and expectations, ensuring high performance and productivity, ensuring effective customer service and education, and evaluating performance

Promote Information Systems Security Awareness throughout the enterprise

To provide security related services and share awareness of information security issues throughout the University the CSO will:

- a. Oversee information security risk assessments for departments or under the direction of IT management and/or Internal Audit
- b. Provide information for security training to employees, contractors or other third-parties that may interact with University information systems and networks.
- c. Conduct workshops or other forums to share security-related topics with service providers, key stakeholders, and the University community

- d. Develop materials and programs to promote security awareness and knowledge

Direct Incident Response

In response to security breaches, the CSO will:

- a. Develop and maintain response procedures and awareness
- b. Mobilize and manage the response team to ensure effective incident response handling
- c. Oversee the risk assessment and resolution
- d. Ensure effective incident response
- e. Determine and implement needed mitigation
- f. Report on incidents, response, resolution, and mitigation

Oversee Information System Access and Security

In relation to the Banner system and related databases, the CSO will:

- a. Work with the director of administrative systems to ensure confidentiality, integrity, and availability of administrative information
- b. Oversee the granting and revocation of database roles, table access, and or other database privileges, often in collaboration with DBA team
- c. Provide consultation on new / changing Banner business processes and their security implications
- d. Using established audit guidelines for segregation of duties and compensating controls, suggest appropriate business process development

5. Work areas or assignments.

(Describe areas over which the employee exercises independent authority, judgment, initiative and discretion)

- a) This position is under the general direction of the Chief Information Officer who provides primarily strategic-level input. Most activities are self-generated from position responsibilities. This position exercises broad discretion in the integration of departmental goals and policies, code and statutory requirements, professional practice and ethics.
- b) This position plays a strategic role in the efficient management of security resources and oversight of enterprise security practices in support of the mission of the University.
- c) This position has full authority to speak and act on behalf of those ITC projects and programs under his or her direction and may speak on behalf of ITC, the division, or University under the guidance of the CIO or appropriate level division/University administrator, often communicating with the University's IT advisory councils on security matters.
- d) This position has broad discretion in exercising independent judgment and initiative over security management, working with departments, agencies, governance councils, and affiliate campuses to explain, justify, and promote operational procedures. Communication skills are often used to exchange

abstract ideas, defend, change/persuade, or deliberate security issues and operational changes.

- e) This position has broad discretion in exercising independent judgment and initiative over security resource management, communicating and working closely with departments, agencies, governance councils, and affiliate campuses to ensure compliance with government regulations and University policy.
- f) This position works independently, exercising initiative and discretion, with numerous and varied stakeholders from the four MSU campuses to share ideas, resolve problems, recommend policy, procedure, and program changes and implementation plans.

6. Extent to which the person in this position is responsible for:

developing & implementing policies

establishing goals for the work unit and/or University

control of personnel use, equipment and/or funds

Policy development and implementation:

- a) Determines need for, writes, develops, vets, and guides the approval process in formulating policies, priorities and goals for IT security on four campuses.
- b) Ensures that associated guidelines and standards are published and reviewed, reviews comments, assists in awareness and enforcement
- c) Shares responsibility with the other ITC senior managers for formulating and implementing related changes.

Establishment of goals for the unit and University:

- a) Has independent responsibility for establishing the short- and long-term goals and objectives for the security operations within the unit.
- b) Has influential responsibility over the establishment of short- and long-term goals and objectives of the University.
- c) Collaborates with the other ITC senior managers in establishing the long-term goals and objectives for ITC overall.

Control of personnel use, equipment and/or funds:

- a) Manages the activities of 2 or more FTE in Security Analyst and Security Associate positions.
- b) Participates in overseeing the security of enterprise-wide infrastructure equipment including servers and network equipment, and desktop equipment throughout the Bozeman campus.

7. Minimum educational and experience requirements for the position.

(Include specialized training or supervisory experience required, as well as applicable professional certification or licenses.)

Bachelor's degree.

Thorough knowledge of security strategies and best practices of the industry.

Relevant understanding of government regulations such as GLB Act, FERPA, HIPPA, etc.

Experience in developing and delivering informational and instructional programs to a diverse audience.

Excellent interpersonal, communication, and negotiation skills.

A record of successful leadership in planning and implementing technological initiatives.

8. Required and Preferred Qualifications

("Required qualifications" refers to the minimum and "must have" education and experience standards for an applicant to be considered. "Preferred qualifications" refers to standards that will improve an employee's ability to perform the duties and responsibilities of the position and enhance their performance.)

Required:

Bachelor's degree in combination with 15 + years of experience in information technology with an emphasis in security.

A history of success at the senior management level.

A record of successful leadership in planning and implementing technological initiatives.

Direct experience managing enterprise-wide information technology security.

Preferred:

Advanced education in Information Technology and security.

Significant accomplishments in the development and delivery of innovative user-focused information technology security programs.

9. Knowledge, Skills and Abilities.

(Focus on results-oriented accomplishments, i.e. skill in use of Microsoft software; ability to work cohesively and productively in a team-oriented environment; knowledge of MSU policies and procedures. etc.)

Knowledge of security strategies and best practices of the industry. Relevant understanding of government

regulations such as GLB Act, FERPA, HIPPA, etc.

Skills in communication and analysis to build understanding of business needs, gather requirements, establish objectives, synthesize plans, and clearly articulate issues, plans, risks, and mitigation to constituents and stakeholders.

Skills in the development and public presentation of informative, relevant, and meaningful presentations on related security topics.

Knowledge and demonstrated experience in implementation and management of business information systems, integration and migration. Knowledge of basic quality improvement processes and ability to apply these processes for effective process improvement, including business process analysis, workflow analysis, audit control, segregation of duties, compensating controls, and other audit guidelines.

Skills in staff supervision, coaching, mentoring, and task delegation.

Ability to work influentially within the culture and governing structure of a higher education institution, including working interdependently with security stakeholders across the enterprise and across a wide range of skills and authority.

Ability to lead working committees / teams by effectively organizing, setting agendas, prioritizing topics, developing goals, creating action plans, delegating work, developing project and task plans, measuring / reporting progress, and facilitating discussion and/or issue resolution.

Ability to research and formulate strategies and tactics appropriate for this institution to mitigate security, disaster, and business continuity risks.

Ability to lead response team by facilitating the efforts to: define the problem or incident, assess the risk and exposure, create plans to resolve, prioritize actions, and resolve issues that may arise, and document appropriately. Ability to communicate an effective incident report to University management summarizing the incident, the impacts on the organization, and steps taken to resolve.

10. Additional Information

(List any unusual requirements for the position such as: repetitive movements; extensive standing or sitting; lifting requirements; possess or have the ability to obtain a Montana Drivers License, etc.)

