

Position Summary

Under the direction of the Bureau of Security director, this position provides leadership and technical expertise to the security compliance, audit and awareness team. This position is responsible for auditing data security, and ensuring compliance in regulations (e.g. Criminal Justice Information Services (CJIS), Family Educational Rights and Privacy Act (FERPA), Federal Information Security Management Act (FISMA), Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Social Security Administration (SSA), etc.) surrounding the Executive Branch agencies information systems hosted by the Division of Enterprise Technology. In addition, this position manages a security awareness program to ensure that employees have the information and training they need to help protect state and residents' data.

This position will coordinate the security compliance, audit and awareness team activities to ensure that state-wide policies, programs, and principles are implemented, measured, and continually improved for greater organizational effectiveness.

Goals and Worker Activities

A. 40% Manage, direct, and supervise the security compliance, audit and awareness team.

1. Manage the recruitment and hiring process for applicants; ensure that hiring decisions are made in accordance with department policies including affirmative action and equal employment opportunity guidelines.
2. Recommend and initiate personnel actions such as reclassification, reallocation, competitive promotion as needed to ensure appropriate and effective allocation of staff resources and compensation.
3. Implement and provide information about affirmative action policies and procedures, harassment and discrimination policies, and advancement opportunities for all staff.
4. Evaluate employee performance, coach employees, acknowledge or provide formal recognition for good performance, recommend pay increases and/or promotions where warranted, and take appropriate disciplinary action, and resolve grievances as needed.
5. Oversee the development of training and career development programs for all employees.
6. Prioritize the work of team members of the security compliance, audit and awareness.

B. 20% Ensure compliance with regulatory and other industry standards for infrastructure services provided by the Division.

1. Catalog the internal and external policies, standards and regulations that govern regulatory compliance.

2. Partner with other Federal and State agencies to develop strategic security policy and controls that meet regulatory compliance consistently across all State agencies.
3. Create, publish and utilize metrics that can be used to demonstrate compliance and or compliance gaps.
4. Establish and maintain communication and remediation plans for regulatory compliance issues.
5. Audit and report on the effectiveness of security controls.
6. Prepare reports that are required to meet regulatory compliance audits.

C. 20% Manage the State's security awareness program.

1. Lead cross-functional teams in needs assessment, design, or implementation projects to address security awareness training needs..
2. Develop and manage awareness training programs for all State employees as well as specific groups such as software developers.
3. Develop and maintain other security awareness informational materials and web content.
4. Evaluate, test and measure the effectiveness of the security awareness program.

D. 15% Research and Development of Security technologies

1. Lead research and fiscal analysis on the best methods for meeting information technology security needs; advise the DOA management and customer management at other State agencies.
2. Estimate the effects on Division, and Department plans for personnel, equipment, materials and processes.
3. Lead the testing and evaluation of emerging technologies as they become available. Evaluate and assess the impact on DET-hosted systems. Determine technology limitations.
4. Lead researching of solutions for significant changes in the security infrastructure. Present recommendations to the bureau of security director.
5. Recommend improved methods and technologies to manage the security infrastructure and to become more efficient and effective.

E. 5% Professional development

1. Attend seminars and other educational opportunities; interact with counterparts at other organizations and read professional journals and magazines.
2. Maintain close interaction with IT and security staff at other government agencies and private sector organizations.

Knowledge and Skills

1. Expert knowledge of federal, state and regulatory laws and standards for securing systems (e.g. NIST, HIPAA, PCI, CJIS, etc.).
2. Knowledge in network protocols, information technology security and firewalls, encryption, authorization and authentication technologies
3. Demonstrated ability to conceptualize and articulate IT solutions in plain language to IT and the non-IT people.
4. Demonstrated outstanding leadership including in facilitating diverse groups of individuals to collaboratively achieve consensus
5. Proactive, detail-focused problem solving skills
6. Demonstrated knowledge of network environments and security issues
7. Demonstrated ability to effectively plan and control projects
8. Knowledge of project management tools and methodologies
9. Knowledge of cost benefit analyses and feasibility study techniques
10. Knowledge of the principles of organization, administration and management and developing long and short term goals
11. Knowledge of state and federal employment laws, policies and procedures pertaining to the hiring of new employees including Affirmative Action, Equal Employment Opportunity, and state classified service rules
12. Knowledge of techniques and theory required to manage and supervise professional technical support staff
13. Knowledge of techniques used to establish and maintain effective working relationships with staff and customers
14. Knowledge of effective methods of written and oral communication, including leading and facilitating meetings
15. Knowledge of effective consulting and negotiation practices
16. Knowledge of budgeting, marketing, organizational planning and purchasing principles
17. Excellent interpersonal, communication, and presentation skills are required with a high degree of energy, initiative, and organizational ability
18. A practiced understanding of the 10 Domains of Information Systems Security Professional (CISSP) or other comparable certifications
19. Developing/evolving security standards or protocols
20. Knowledge of audit procedures
21. Knowledge of disaster preparedness and recovery methodologies
22. Knowledge of developing and implementing security and IT policies