

## **Position Summary**

Under the direction of the Bureau of Security director, this position provides leadership and technical expertise to the security operations team. The security operations team is responsible for managing cyber security incidents for the enterprise, ensuring they are properly identified, analyzed, communicated, actioned/defended, investigated and reported. This position will provide leadership for:

- gaining situational awareness through continuous monitoring of networks and other IT assets for signs of attack, anomalies, and inappropriate activities
- determining the cause, scope, and impact of incidents to stop unwanted activity, limit damage, and prevent recurrence
- continuously identifying and remediating vulnerabilities before they can be exploited
- separating and controlling access to different networks with different threat levels and sets of users to reduce the number of successful attacks
- protecting information on computers that routinely interact with untrusted devices on the internet or may be prone to loss or theft

This position will coordinate the security operations team activities with managed security service provider(s) to ensure that division-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 operations team.

1. Develop and maintain the detection, containment, remediation and communication processes for the security operations team and ensure the processes are understood and followed by the team.
2. 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.
3. Recommend and initiate personnel actions such as reclassification, reallocation, competitive promotion as needed to ensure appropriate and effective allocation of staff resources and compensation.
4. Implement and provide information about affirmative action policies and procedures, harassment and discrimination policies, and advancement opportunities for all staff.
5. 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.
6. Oversee the development of training and career development programs for all employees.

7. Prioritize the work of team members of the security operations team.

B. 20% Monitor, measure and communicate threat information.

1. Partner with other federal, state and local agencies to develop strategic security policy and process for information sharing and incident response.
2. Create, publish and utilize metrics to manage the security operations effectively.
3. Establish and maintain communication plans for situational awareness information related to incidents, threats, and vulnerabilities.
4. Prepare presentations and promotional information for the purpose of information security situational awareness.

C. 20% Lead information technology security initiatives

1. Lead cross-functional teams in needs assessment, design, or implementation projects to address security needs.
2. Review internal project study requests and project plans for compliance with IT security strategic goals.
3. Evaluate customer requirements to determine which security solutions best meet needs. Provide cost-benefit analyses as needed and solicit funding to develop and implement new projects and services.
4. Provide information technology security expertise to system developers, system administrators, project managers and other IT professionals to ensure adequate security controls in IT systems.

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 in network protocols, information technology security and firewalls, encryption, authorization and authentication technologies
2. Demonstrated ability to conceptualize and articulate IT solutions in plain language to IT and the non-IT people.
3. Demonstrated outstanding leadership including in facilitating diverse groups of individuals to collaboratively achieve consensus
4. Proactive, detail-focused problem solving skills
5. Demonstrated knowledge of network environments and security issues
6. Demonstrated ability to effectively plan and control projects
7. Knowledge of project management tools and methodologies
8. Knowledge of cost benefit analyses and feasibility study techniques
9. Knowledge of the principles of organization, administration and management and developing long and short term goals
10. 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
11. Knowledge of techniques and theory required to manage and supervise professional technical support staff
12. .
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. An understanding of federal, state and regulatory laws and standards for securing systems. For example, NIST, HIPAA, PCI, CJIS, etc.
20. Developing/evolving security standards or protocols
21. Knowledge of audit procedures
22. Knowledge of disaster preparedness and recovery methodologies
23. Knowledge of developing and implementing security and IT policies