BUTTE-GLENN COMMUNITY COLLEGE DISTRICT

CLASS TITLE: SECURITY MANAGER, INFORMATION TECHNOLOGY L207.100

BASIC FUNCTION: Under the direction of an administrator, manages the daily activities and resources related to information technology network systems team and systems security. Participates in the design and management of network and desktop services, equipment and supplies. The Security Manager, Information Technology position secures the District's information technology resources by monitoring security systems to identify, troubleshoot, diagnose, resolve, and report security problems and breaches. In addition, the position assists in coordinating and conducting investigations involving District technology resources, coordinates information security training, and serves a key role on the District's data breach incident response team. This position will report directly to the Chief Technology Officer (CTO) and works closely with other departmental managers. Performs other related duties as required.

REPRESENTATIVE DUTIES: ***(The duties recorded below are representative of the duties of the class and are not intended to cover all the duties performed by incumbent(s) of any particular position. The omission of specific statements of duties does not exclude them from the position if the scope of work is similar, related or a logical assignment to this class. The essential duties of the class are indicated with an asterisk *.)***

1. In coordination with the CTO, plans for and provides effective and efficient support for District information technology, data systems, networks, and related Information Technology infrastructure, including local area and wide area networks, inter-building and intra-building cable plant; develops new system capabilities to improve overall District technology security operations in the above areas. *

2. Manages assigned technical staff; duties include instructing, assigning, and planning work, determining performance objectives, maintaining standards, coordinating activities, selecting new employees, acting on employee problems and recommending employee discipline and discharge as appropriate. Reviews and evaluates the work of employees for effectiveness, completeness, accuracy, and adherence to departmental policies; offers training, advice and assistance. *

3. Participates in the development, implementation and maintenance of the departmental budget(s) and maintains budget records as required. *

4. Directs and deploys departmental resources to implement projects and programs. *

5. Consults with District administrators, faculty and staff to determine needs and expectations in the secure use and implementation of technology systems and services; research project feasibility, product cost and availability, budgetary allowances and other factors in project planning and design. *

6. Identifies potential threats to safeguard District information security. Provides and assists in recommendations for security roadmap planning and activities. *

7. Responsible for the correct installation and guidance in the management of security appliances, servers, mobile device management, network infrastructure, patch management, and updates. Includes creating processes that align with security best practices.*

8. Prepare reports and or presentation regarding security breaches and extent of real or potential damage. *

9. Install and assist with software and program installations, upgrades and updates. *

10. Conduct testing or simulated cyber-attacks to identify system vulnerabilities. *

11. Leads in the construction and implementation of the Districts cyber security plans and road map. *

12. Provides incident response and remediation support by serving as the technical lead with security vendors, investigators, and law enforcement agencies to support investigation processes. *

13. Assists the District in updating policies, procedures, standards, and practices to increase the District's information security posture. Assures District is complying with safe data collection and storage*

14. Researches emerging security risks and recommends mitigating risk strategies. Implements and aggregates server, network, application, and firewall logs to identify or respond to security vulnerabilities or security incidents. *

15. Conducts periodic audits/risk assessments to develop corrective action plans. Reviews new software and technology solutions to ensure they meet the Districts information security policies, procedures and standards as required by the District's software and technology review process. *

16. Leads and or participates in the review of software licensing, contracts, and accessibility requirements. Creates plans, guides projects and leads teams in addressing security related issues and objectives.*

17. Performs security design/review using flowcharts/diagrams to review applications, network and server, architecture and ensure secure deployments on-premise or in the cloud. *

18. Assists the District's Business Contracts and Risk Management Department with developing bid specifications for software or hardware to identify criteria needed to meet the District's information security standards as required by the District's procurement policies and procedures. *

19. Researches information technology security trends, new products/services to provide recommendations to the CTO in the continued improvement and support of the District's technology infrastructure and the District's overall state of cybersecurity readiness. *

20. Identifies, assesses, and recommends information security training resources for District employees and District students by reviewing security incidents and their root causes. *

21. Provide, perform, and coordinate security related trainings for management, classified and faculty staff, and students. *

22. Collaborates and works with outside agencies, vendors, and contractors in security infrastructure and operations.

23. Serves on a variety of District committees as requested.

24. Performs related work as required.

MINIMUM QUALIFICATIONS:

EDUCATION AND EXPERIENCE:

- Associate's Degree or the equivalent in Information Technology, Computer Science or Management Information Systems or a related field; **AND**
- Five (5) years of experience developing, implementing, and maintaining information technology security systems.

** Associate's Degree education equivalency equals two (2) years of increasingly responsible related work experience for each full year (24-30 units) of college. Work experience must be in an office setting.*

CERTIFICATES, LICENSES, REGISTRATION AND OTHER REQUIREMENTS:

- Hold and maintain a valid driver's license throughout duration of employment with the District.
- Some travel may be required.

DESIRED QUALIFICATIONS:

- Bachelor's Degree in Computer Science, Computer Information Systems, Management Information Systems.
- Computer and network security certifications, courses, and trainings in a technology related field or the equivalent

CERTIFICATES, LICENSES, REGISTRATION AND OTHER REQUIREMENTS:

- CompTIA Security +
- Certified Information Systems Security Professional (CISSP)
- ISACA Certified Information Security Manager (CISM)
- EC-Council Certified Ethical Hacker (CEHv11)

KNOWLEDGE, SKILLS AND ABILITIES: *(May be acquired through education, training, and/or experience.)*

Knowledge of: District policies and procedures; System Incident Management software to identify security vulnerabilities and respond to security incidents; The Health Insurance Portability and Accountability Act (HIPPA), the Payment Card Industry Data Security Standards (PCI DSS), the Family Educational Rights and Privacy Act (FERPA), System and Organization Controls (SOC), and ISO 27001 to conduct periodic audits and develop corrective action plans; Vulnerability scanning tools to identify vulnerabilities in network based assets such as firewalls, routers, web servers, application servers, etc.; Penetration testing computer programs to identify vulnerabilities in District computer programs and to develop mitigation strategies; Center for Internet Security (CIS) Controls to eliminate the District's online vulnerabilities and secure the District from online security threats; Current emerging technology and security threats to assist in updating security standards and policies and procedures; Microsoft Office Suite software to communicate with a variety of individuals involved on the security incident response team; New information security products and services to make recommendations that will protect District applications.

Ability to: interpret and apply District policies, rules and procedures; compose correspondence and reports; coordinate and provide leadership to assigned personnel; Conduct periodic audits and develop corrective action plans; perform security audits/risk assessments to safeguard information; Use computer software to develop flowcharts and diagrams to track and review information technology functions; Work collaboratively with District staff to develop bid specifications for the procurement of hardware; Work collaboratively with District staff to update policies, procedures, standards, and practices in order eliminate security information threats to the District; Maintain confidentiality during the course of an investigation; Analyze current situations related to information security and make recommendations to departmental and District management; Conduct research in order to develop strategies that will combat security risks that stem from new technology; Analyze information security incidents to determine their root causes and develop training resources to develop preventative practices; Coordinate security awareness trainings to create awareness of security issues; Safely operate a vehicle for travel; Strong collaboration skills.

WORK DIRECTION, LEAD AND SUPERVISORY RESPONSIBILITIES:

Provides direct supervision to regular and short-term classified employees.

PHYSICAL EFFORT:

Normal office environment.

CONTACTS:

Faculty, staff, administrators, students, employers, government agencies and the general public.

WORKING CONDITIONS:

Normal office environment.

NOTE: THIS CLASS IS EXEMPT UNDER FLSA PROVISIONS