Board Approved March 25, 2015
FLSA: EXEMPT

ASSISTANT DIRECTOR, INFRASTRUCTURE AND DATA SECURITY

DEFINITION

Under administrative direction, plans, organizes, manages, and provides direction and oversight for all functions and activities related to network and data security for the District; plans, designs, and provides direction and oversight for the network infrastructure, including wireless systems; provides highly complex and responsible support to the Director, Academic Technology and Infrastructure & Deputy Chief Technology Officer in areas of expertise.

SUPERVISION RECEIVED AND EXERCISED

Receives administrative direction from the Director, Academic Technology and Infrastructure & Deputy Chief Technology Officer. Exercises direct and general supervision over technical staff.

CLASS CHARACTERISTICS

This is an Assistant Director classification in the Information Technology Department that manages all activities of information security operations and activities. Responsibilities include performing diverse, specialized, and complex work involving significant accountability and decision-making responsibility. The incumbent organizes and oversees day-to-day activities and is responsible for providing professional-level support to the Director, Academic Technology and Infrastructure & Deputy Chief Technology Officer in a variety of areas. Assists in short- and long-term planning and development and administration of departmental policies, procedures, and services. Successful performance of the work requires an extensive professional background, as well as, skill in coordinating departmental work with that of other departments. This class is distinguished from the Director, Academic Technology and Infrastructure & Deputy Chief Technology Officer in that the latter has overall responsibility for all functions of the Academic and Infrastructure unit and for developing, implementing, and interpreting public policy.

EXAMPLES OF ESSENTIAL FUNCTIONS (Illustrative Only)

- Plans, manages, and oversees the daily functions, operations, and activities related to network and data security, including policy review and creation, perimeter and internal firewalls, intrusion detection and prevention, virtual private network (VPN) access, vulnerability identification and assessment, patch management, security log auditing, compliance with applicable laws and regulations such as Peripheral Component Interconnect (PCI) and the Family Education Rights and Privacy Act (FERPA), forensic analysis, and incident response and assessment.
- Manages and participates in the development and implementation of goals, objectives, policies, and priorities for District-wide information security; assists in defining overall network design and data security strategies and procedures.
- Monitors and evaluates the efficiency and effectiveness of security policies, processes, and procedures; identifies opportunities for improvement and makes recommendations to the Director, Academic Technology and Infrastructure; develops and standardizes procedures and methods to improve information security operations; implements appropriate additions, changes, updates and revisions.
- Participates in the selection of, trains, motivates and evaluates assigned personnel; works with employees on performance issues; recommends discipline to the Director, Academic Technology and Infrastructure.
- Implements security and network management systems to track and monitor network traffic to identify and report on network attacks, potential network disruptions and identify network anomalies that should generate alerts and response.

- Monitors and evaluates the efficiency and effectiveness of security systems; reviews logs for potential security threats, reviews systems for unusual server or network behavior; scans infrastructure to identify vulnerable computers, servers, and network equipment; audits servers for appropriate patches and service efficiencies; audits commercial and open source web applications and tests custom web applications for security vulnerabilities.
- Identifies where personally identifiable information (PII) is stored and mitigates its loss with whole disk encryption.
- Provides leadership and participates effectively with Information Technology staff in network design and engineering to ensure appropriate levels of security are in place and maintained; evaluates new technology for security threats.
- Monitors, evaluates, and analyzes existing network design; make recommendations for short and long term design and equipment updates to ensure service redundancy, security, and technical currency.
- Works with staff District-wide to investigate and perform security forensics related to any possible public safety, human resources, or security issues or breeches.
- Develops and documents strategies to mitigate network attacks and breeches, including malware, social engineering, and spam/phishing.
- Advises, provides guidance, and prepares and delivers presentations on issues pertaining to information security.
- Monitors changes in regulations and technology that may affect assigned functions and operations, including those specific to privacy and the protection of critical personal data; implements policy and procedural changes; ensures that relevant regulations are adhered to.
- Participates in strategic technology planning with focus on ensuring network capabilities support current and emerging technologies related to enhanced instruction, distance education, student services, and administrative system needs; provides guidance and advocacy regarding prioritization of infrastructure investments that impact network design and data security.
- Integrates network design and network security initiatives including network enhancements network encryption, firewall, VPN, and DMZ infrastructure.
- Develops and designs security strategies to implement a secure college-wide wireless infrastructure to support Students Services, Instruction, and Administrative requirements.
- Advises management of risk issues that are related to information and data security issues and recommends actions in support of the District's wider risk management programs.
- Attends and participates in professional group meetings and various committees and advisory groups; stays abreast of new trends and innovations in network and data security.
- Prepares, reviews, and presents staff reports, various management and information updates, and reports on special projects as assigned by the Director, Academic Technology and Infrastructure.
- Learns and applies emerging technologies and, as necessary, to perform duties in an efficient, organized, and timely manner.
- Provides a working and learning environment that is free from prohibited discrimination, harassment and retaliation (DHR), and provided by applicable law and District policies. Attends District mandated DHR training and participates in DHR investigations as directed. Prevents discrimination and harassment and retaliation against individuals who bring these complaints forward through recognizing and reporting possible incidents to the Director of Equal Employment Opportunity Programs in Human Resources.
- Performs other related duties as assigned.

QUALIFICATIONS

Knowledge of:

- Administrative principles and practices, including goal setting, program development, implementation, and evaluation.

- Principles and practices of employee supervision, including work planning, assignment, review and evaluation, and the training of staff in work procedures.
- Network design in a campus-wide environment, including required resilience, redundancy, and security to support Instructional Technology, Campus Portal Systems, Distance Education, Student Services, and Enterprise Administrative Systems.
- Operational characteristics of TCP/IP and LAN administration, Microsoft Windows, Linux/Unix, AIX, and large scale Database Management Systems.
- IPSEC, Intranet, Internet, and Wide Area Network technologies, operations, and security.
- Network routing and switching at Layer 1 – 7, including design and management of layer 3 networks in a large scale campus/multi-location environment.
- Principles and practices of firewall implementation, maintenance, VPN, and remote access strategies and security protocols.
- Methods and techniques of network monitoring, network management, intrusion detection, DoS prevention, computer and network forensics.
- Wireless technologies, both licensed and unlicensed, including protocols, security, application and implementation.
- Network design and management in support of state-of-the-art Instructional, Distance Education, Student Services, Web Portal, Administrative, and Imaging Systems.
- Network based collaboration environments such as Lotus Domino/WebSphere, Sametime, Macromedia Breeze, Video Streaming, uPortal, and others.
- Network design and management in support of an Oracle RDBMS environment.
- Critical security issues, tools, and techniques related to interactive e-commerce web applications.
- Applicable Federal, State, and local laws, regulatory codes, ordinances, and procedures relevant to assigned programs, projects, and operations.
- Methods and techniques for the development of presentations, business correspondence, and information distribution; research and reporting methods, techniques, and procedures.
- Principles and procedures of record keeping.
- Modern office practices, methods, and computer equipment and applications.
- English usage, spelling, vocabulary, grammar, and punctuation.
- Techniques for effectively representing the District in contacts with various business, professional, educational, regulatory, and legislative organizations.
- Techniques for providing a high level of customer service by effectively dealing with the public, vendors, students, and District staff, including individuals of various ages, disabilities, socio-economic and ethnic groups.

Skills & Abilities to:

- Develop and implement goals, objectives, policies, procedures, work standards, and internal controls for assigned program areas.
- Provide administrative and professional leadership and direction for assigned operations and activities.
- Participate in the design, management, and security of a comprehensive, District-wide, state-of-the-art network infrastructure/services.
- Perform technical specification, design, implementation, and integration on network services in support of Instructional, Student Services, Administrative, and Community Support initiatives and goals.
- Analyze problems, identify alternative solutions, project consequences of proposed actions, and implement recommendations in support of goals.
- Research, analyze, and evaluate new network technologies and service delivery methods and techniques.
- Participate in the development and administration of technical network/infrastructure goals, objectives, and procedures.

- Establish and maintain effective working relationships with those contacted in the course of work.
- Organize and provide leadership to workgroups consisting of a broad range of stakeholders related to network and security initiatives.
- Interpret, apply, explain, and ensure compliance with Federal, State, and local policies, procedures, laws, and regulations.
- Plan, organize, direct, and coordinate the work of supervisory, professional, and technical personnel; delegate authority and responsibility.
- Select, motivate, and evaluate the work of staff and train staff in work procedures.
- Effectively represent the District and the department in meetings with various educational, business, professional, regulatory, and legislative organizations.
- Prepare clear and concise reports, correspondence, policies, procedures, and other written materials.
- Establish and maintain a variety of filing, record keeping, and tracking systems.
- Organize and prioritize a variety of projects and multiple tasks in an effective and timely manner; organize own work, set priorities, and meet critical time deadlines.
- Operate modern office equipment including computer equipment and specialized software applications programs.
- Use English effectively to communicate in person, over the telephone, and in writing.
- Understand scope of authority in making independent decisions.
- Review situations accurately and determine appropriate course of action using judgment according to established policies and procedures.
- Establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.

Education and Experience:
Any combination of training and experience which would provide the required knowledge, skills, and abilities is qualifying. A typical way to obtain the required qualifications would be:

Equivalent to graduation from a regionally accredited four-year college or university with major coursework in data security, computer science, management information systems, or a related field and five (5) years of experience as a network administrator, including supervisory experience.

Licenses and Certifications:

- Possession of, or ability to obtain, a valid California Driver's License by time of appointment.
- Certified Information Systems Security Professional (CISSP) preferred.

PHYSICAL DEMANDS

Must possess mobility to work in a standard office setting and use standard office equipment, including a computer; to operate a motor vehicle and to visit various District and meeting sites; vision to read printed materials and a computer screen; and hearing and speech to communicate in person, before groups, and over the telephone. This is primarily a sedentary office classification although standing and walking between work areas is be required. Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment. Positions in this classification occasionally bend, stoop, kneel, reach, push, and pull drawers open and closed to retrieve and file information. Employees must possess the ability to lift, carry, materials and objects up to 50 pounds.

ENVIRONMENTAL ELEMENTS

Employees work in an office environment is exposed to loud noise levels, cold temperatures, dust and allergens. Employees may interact with staff and/or public and private representatives and contractors in interpreting and enforcing departmental policies and procedures.