Orange County Department of Education
Human Resources Department
Classified Management Class Specification

Cyber Security Manager | **Class Code: 1600**
Work Days: 225

GENERAL PURPOSE

Develop, implement, monitor, and maintain cyber security programs for the Orange County Department of Education (OCDE) and for Orange County school districts; identify and address critical systems and critical digital assets; maintain cyber security attack mitigation and incident response capability; and provide assistance to senior level management staff.

SUPERVISION RECEIVED AND EXERCISED

1. Receives general supervision from higher level management staff.
2. May exercise direct supervision over professional, and/or technical staff.

ESSENTIAL DUTIES AND RESPONSIBILITIES

This position description is intended to describe the general nature and level of work performed by an employee assigned to this position. This description is not an exhaustive list of all duties, responsibilities, knowledge, skills, abilities, and working conditions associated with this position. All requirements are subject to possible modification to reasonably accommodate individuals with a disability.

1. Lead the development and assist in the implementation of cybersecurity goals, objectives, and strategic plan; establish schedules and methods for providing specialized cybersecurity services; implement cybersecurity policies and procedures for OCDE.
2. Contribute to the development and improvement of security monitoring and incident response processes and solutions as required to support cyber security program for OCDE and school districts.
3. Provide a coordinated response to complex cyber-attacks; identify threats and develop suitable defense measures, evaluate system changes for security implications, and recommend enhancements; research and draft cyber security white papers.
4. Operate security monitoring and incident response toolsets with a focus on continuous improvement; monitor for attacks, intrusions, vulnerabilities, and risks.
5. Interface with outside law enforcement agencies on electronic security breaches.
6. Research and recommend solutions for incident response and digital forensics.

ESSENTIAL FUNCTION STATEMENTS (cont.):

7. Run vulnerability valuation and review protocols, hardware, and software for OCDE and school districts.
8. Develop, implement and facilitate cybersecurity user trainings for OCDE and school district personnel.
9. Establish, oversee, and incorporate current and emerging electronic information security technologies, security issues and information privacy legislation and regulations and incorporate changes to IT policies, standards and procedures.
10. Provide recommendations and guidance to districts to build in security during the development stages of software systems, networks, and data centers.
11. Keep up-to-date on emerging cyber security technologies and methodologies.
12. Demonstrate attendance sufficient to complete the duties of the position as required.
13. Perform related duties similar to the above in scope and function as required.

QUALIFICATIONS (KNOWLEDGE, SKILL, ABILITY REQUIREMENTS)

Knowledge of:

1. Leadership and supervision; project management; and strategic technology planning, execution and IT policy development related to security.
2. Principles and practices of application architecture, cyber security, networks, servers, databases, and analysis.
3. Federal Rules of Civil Procedure (FRCP), e-discovery, Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Children's Internet Protection Act (CIPA), Payment Card Industry Data Security Standard (PCI DSS), and other information security related laws and regulations.
4. Information Technology Security Risk assessment methods and techniques.
5. Cyber defense methodology and technology.
6. Authentication, authorization, and encryption technologies.
7. Methods and techniques of evaluating business requirements and developing information systems solutions.
8. Principles and practices of programming languages, servers, databases, operating systems, networks, TCP/IP protocols, and related technology.
9. Procedures, methods, and techniques of project and workflow management and organization.

Ability and Skill to:

1. Effectively manage multiple projects and provide accurate, clear and timely information using multiple communications media.

Ability and Skill to (cont):

2. Act as a change agent to facilitate improvement in information security.
3. Interpret the organizational and division strategic plan and create relevant goals and plans for assigned areas.
4. Effectively adapt and adjust program services to meet changing priorities and customer-specific needs.
5. Establish and maintain effective working relationships with various constituencies.
6. Interpret and explain laws, codes, contracts, policies, and procedures.
7. Develop and present training materials.
8. Prepare clear and concise correspondence, reports, and other written materials.
9. Analyze problems, identify alternative solutions, project consequences of proposed actions, and implement recommendations in support of goals.
10. Communicate clearly and concisely, both orally and in writing, in English; present information effectively in front of both large and small groups.

Education, Training, and Experience:

A typical way of obtaining the knowledge, skills, and abilities outlined above is Bachelor's degree from an accredited college or university with major course work in information security or a related field and experience in information security technology, specifically with penetration testing, intrusion detection, incident response, or digital forensics and five years working in a technical capacity in any of the following areas: cybersecurity, networking, application development, databases, servers; three years in an educational agency; and at least one year experience in managing in a technical capacity.

PHYSICAL AND MENTAL DEMANDS

The physical and mental demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this class. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Physical Demands

While performing the duties of this job, employees are regularly required to bend, stoop, push, pull, grasp, squat, twist, kneel, walk, sit, and reach to access materials or equipment and complete other tasks as assigned; lift and carry up to 25 pounds; and lift from ground, waist, chest, shoulder, and above shoulder level. The position may include occasional need to traverse uneven surfaces.

Employees in this classification are to be able to travel countywide to a variety of sites within a reasonable time frame; read written and electronic materials; communicate clearly in person, on the phone, and via email; and operate all required equipment.

Mental Demands

While performing the duties of this class, employees are regularly required to use written and oral communication skills; read and interpret information; analyze and solve problems; use mathematical reasoning; make observations; learn and apply new information or skills; perform highly detailed work; work on multiple, concurrent tasks with frequent interruptions; work under intensive deadlines and meet productivity requirements; and interact successfully with various groups of people encountered in the course of work.

WORK ENVIRONMENT

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this class. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Employee typically works in an office environment that is fast paced with high pressure.

5/2024