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

Cyber Security Strategist **Class Code: 1679**
Work Days: 225

GENERAL PURPOSE

Manage, plan, organize, and supervise cyber security services within the Information Technology Division; coordinate assigned activities with other divisions and outside agencies; and provide assistance to higher 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 being 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. Recommend and assist in the implementation of goals, objectives, and strategic plan; establish schedules and methods for providing specialized services; and implement policies and procedures.
2. Manage, plan, organize, and supervise cyber security services within the Information Technology Division.
3. Monitor and evaluate the efficiency and effectiveness of service delivery methods and procedures and recommend, within division policy, appropriate service and staffing levels.
4. Review, investigate, and evaluate new technologies for current and future needs; ensure that all technologies comply with OCDE standards and strategic direction.
5. Select, train, plan the work of, supervise, and evaluate staff; provide coaching to employees; collaborate on goal development; set clear expectations; provide constructive feedback; assist in improvement as needed; and check in regularly for understanding.
6. Develop and maintain project schedules; plan, organize, coordinate, schedule, and track project tasks and milestones.
7. Conduct meetings with customers and transform requirements into effective applications.
8. Attend and participate in professional group meetings; stay abreast of new trends and innovations.
9. Generate documentation for staff and training.
10. Contribute to the development and improvement of security monitoring and incident response processes and solutions as required to support cyber security programs for OCDE and school districts.

11. Provide a coordinated response to complex cyber-attacks; identify threats and develop suitable defense measures; evaluate system changes for security implications and recommend enhancements; and research and draft cyber security white papers.
12. Operate security monitoring and incident response toolsets focusing on continuous improvement; monitor for attacks, intrusions, vulnerabilities, and risks.
13. Interface with outside law enforcement agencies on electronic security breaches.
14. Research and recommend solutions for incident response and digital forensics.
15. Run vulnerability valuation and review protocols, hardware, and software for OCDE and school districts.
16. Develop, implement, and facilitate cybersecurity user training for OCDE and school district personnel.
17. 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.
18. Provide recommendations and guidance to districts to build in security during the development stages of software systems, networks, and data centers.
19. Keep up-to-date on emerging cyber security technologies and methodologies.
20. Perform related duties similar to the above in scope and function as required.
21. Demonstrate attendance sufficient to complete the duties of the position as required.

QUALIFICATIONS (KNOWLEDGE, SKILL, ABILITY REQUIREMENTS)

Knowledge of:

1. Principles, practices, methods, and techniques of information systems project management.
2. Principles and practices of program development and administration.
3. Principles and practices of budget preparation and administration.
4. Procedures, methods, and techniques of project and workflow management and organization.
5. Principles of effective supervision, leadership, training, coaching, and performance evaluation.
6. Pertinent federal, state, and local laws, codes, and regulations.
7. Leadership and supervision; project management; and strategic technology planning, execution, and IT policy development related to security.
8. Principles and practices of application architecture, cyber security, networks, servers, databases, and analysis.
9. Federal Rules of Civil Procedure (FRCP), e-discovery, Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Children's Internet Protection Act (CIPA), Payment Card Industry Data Security Standard (PCI DSS), and other information security related laws and regulations.
10. Information Technology Security Risk assessment methods and techniques.
11. Cyber defense methodology and technology.
12. Authentication, authorization, and encryption technologies.
13. Methods and techniques of evaluating business requirements and developing information systems solutions.

14. Principles and practices of programming languages, servers, databases, operating systems, networks, TCP/IP protocols, and related technology.

Ability and Skill to:

1. Select, train, lead, coach, direct the work of, supervise, and evaluate management, supervisory, professional, and technical employees; and effectively delegate authority and responsibility.
2. Interpret the organizational and division strategic plan and create relevant goals and plans for assigned areas.
3. Effectively adapt and adjust program services to meet changing priorities and customer-specific needs.
4. Interpret and apply federal, state, and local laws, codes, and regulations.
5. Provide project oversight and support and manage multiple projects and requests.
6. Establish and maintain effective working relationships with various constituencies.
7. Prepare clear and concise correspondence, reports, and other written materials.
8. Analyze problems, identify alternative solutions, project consequences of proposed actions, and implement recommendations in support of goals.
9. Communicate clearly and concisely, both orally and in writing, in English; and present information effectively in front of both large and small groups.
10. Manage multiple large-scale complex projects.
11. Learn core business concepts and understand how to implement changes and their impact on the application and related business units.
12. Research and evaluate new technology in the assigned area of responsibility.
13. Prepare and administer program budgets.
14. Research, analyze, and evaluate new service delivery methods and techniques.
15. Act as a change agent to facilitate improvement in information security.
16. Serve as project manager on cyber security projects.
17. Develop and present training materials.

Education, Training, and Experience:

A typical way of obtaining the knowledge, skills, and abilities outlined above is a bachelor's degree 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 (5) years working in a technical capacity in any of the following areas: cybersecurity, networking, application development, databases, servers; three (3) years in an educational agency; and at least one (1) year experience in managing in a technical capacity; or an equivalent combination of training and experience.

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.

Physical Demands

Employees must be able to perform the essential functions of the position with or without accommodation. Employees in this classification must be able to travel countywide to a variety of sites within a reasonable time frame, read written and electronic materials, and communicate clearly with those contacted through the course of work (typically in person, on the phone, and via email); perform deskwork for extended periods; and access and operate all required equipment for job duties. The position may include occasional need to traverse uneven surfaces and move items weighing up to 25 pounds.

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.