



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

---

**Cyber Security Analyst**

**Class Code: 1565**

**Work Days: 225**

**GENERAL PURPOSE**

Implement, monitor, and maintain cyber security programs for the Orange County Department of Education (OCDE) and 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 higher level management staff.

**SUPERVISION RECEIVED AND EXERCISED**

Receives general supervision from higher level management 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. 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.
3. Assist in a coordinated response to complex cyber-attacks; identify threats and develop suitable defense measures; evaluate system changes for security implications; and recommend enhancements.
4. Investigate, assess, and document cybersecurity events and incidents.
5. Operate security monitoring and incident response toolsets focusing on continuous improvement; monitor for attacks, intrusions, vulnerabilities, and risks.
6. Conduct research, schedule and conduct meetings, draft reports, and monitor and report on projects as appropriate.
7. Run vulnerability valuation and review protocols, hardware, and software for OCDE and school districts.
8. Develop and facilitate user trainings for OCDE and school district personnel.
9. Provide guidance to districts to build security during the development stages of software systems, networks, and data centers.
10. Prepare and create regular reports to document and process implementation, improvements made, and security breaches that may cause damage to OCDE.
11. Demonstrate attendance sufficient to complete the duties of the position as required.

- 
12. Perform related duties similar to the above in scope and function as required.

## **QUALIFICATIONS (KNOWLEDGE, SKILL, ABILITY REQUIREMENTS)**

### **Knowledge of:**

1. Principles and practices of application architecture, cyber security, networks, servers, databases, and analysis.
2. Cyber defense methodology, technology, and toolsets, including the understanding of firewalls, proxies, SIEM, antivirus, and IDPS concepts.
3. General knowledge of CIS Controls or NIST frameworks.
4. Recent developments, current literature, and sources of information related to cyber security technologies and methodologies.
5. Principles and practices of programming languages, servers, databases, operating systems, networks, TCP/IP protocols, and related technology.
6. Procedures, methods, and techniques of penetration testing, incident report procedures, and data privacy procedures.
7. Principles, methods, and techniques of research.
8. Procedures, methods, and techniques of project and workflow management and organization.

### **Ability and Skill to:**

1. Identify and mitigate network vulnerabilities and explain how to avoid them.
2. Manage multiple competing priorities efficiently and effectively.
3. Establish and maintain effective working relationships with various constituencies.
4. Interpret and explain laws, codes, contracts, policies, and procedures.
5. Develop and present training materials.
6. Prepare clear and concise correspondence, reports, and other written materials.
7. Interpret the organizational and division strategic plan and create relevant goals and plans for assigned areas.
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.

### **Education, Training, and Experience:**

A typical way of obtaining the knowledge, skills, and abilities outlined above is a bachelor's in information security or a related field and one to two years of experience in information security technology, specifically with penetration testing, intrusion detection, incident response, or digital forensics; 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 essential functions.

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