

## **CYBERSECURITY ANALYST**

### **DEFINITION**

Under supervision, monitors and maintains integrated security systems; analyzes overall threats and performance among various enterprise technology platforms, distributed networks and end-user computing devices.

### **SUPERVISION RECEIVED/EXERCISED**

Receives supervision from a Manager or designee. Exercises no supervision.

### **DISTINGUISHING CHARACTERISTICS**

Cybersecurity Analysts provide technical assistance to user departments and staff and conduct the analyses of security threats, system performance, and participates in identifying and resolving more complex operating system issues. This class differs from the Senior Cybersecurity Analyst in that the latter has lead responsibilities and participates in identifying and resolving more complex enterprise technology platform and security issues.

### **EXAMPLES OF IMPORTANT AND ESSENTIAL DUTIES**

May include, but are not limited to, the following:

Provides support with cybersecurity hardware, software and services which may involve the use of distributed networks, local area networks, data transfer between operating systems, cloud services and other types of data networks and services.

Responds to security issues submitted via City ticketing system and other means.

Monitors computer networks for security issues; investigates security breaches and other cybersecurity incidents; and resolves detected vulnerabilities to maintain a high-security standard.

Meets with user departments; provides guidance in analyzing operational technology needs to determine requirements, ensure security of systems and prepares reports of analyses.

Recommends and reviews services, hardware, software, and network configurations to establish the best secure use of resources to meet City needs.

Provides technical assistance in the repair, operation and maintenance of enterprise technology platforms.

Provides installation, evaluation, and diagnosis of enterprise technology platforms.

Recommends modifications for hardware, software, and services.

Performs related duties as required.

## **JOB RELATED AND ESSENTIAL QUALIFICATIONS**

### **Knowledge of:**

Storage Area Networking (SAN) technologies and Network Attached Storage (NAS) equipment.

Microsoft Windows Server and Linux Operating Systems

Local Area Networks (LAN), Wide Area Networks (WAN), Internet and Intranets.

Server virtualization and compute platforms.

Best practices of network security, desktop/server security, data security, forensic Investigation and Identity and Access Management (IAM).

Enterprise grade anti-virus systems

Enterprise grade DNS Filters

Enterprise grade Vulnerability Scanners

### **Ability to:**

Analyze functional network requirements and specifications for computer hardware and software.

Prepare clear, concise, and comprehensive records, reports, correspondence and other written materials.

Direct installation, maintenance, and repair of enterprise technology platforms.

Train and provide support to staff.

Establish and maintain effective working relationships with those contacted in the performance of duties.

Communicate effectively, both orally and in writing.

Adapt to evolving technology to solve problems.

### **Skill to:**

Safely operate a motor vehicle

## **MINIMUM QUALIFICATIONS**

High School Diploma or GED equivalent; and two (2) years of experience in cybersecurity practices.

**Special Requirement**

Possession and continued maintenance of a valid California Driver's License is required at time of appointment.

Candidates selected for hiring consideration I be required to pass an extensive pre-employment background investigation.

APPROVED: \_\_\_\_\_  
                    *(Signature on File)*  
                    Director of Personnel Services

DATE: 7/7/21

NEW:JTC:SCM:bn