SAN BERNARDINO MUNICIPAL WATER DEPARTMENT CLASSIFICATION SPECIFICATION

TITLE: INFORMATION SECURITY ANALYST

DATE: 7/1/2025 **JOB CODE: 2109**

FLSA STATUS: EXEMPT **UNIT REPRESENTATION: MID-MGMT**

Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are not intended to reflect all duties performed within the job.

DUTIES SUMMARY

Under general direction, to design, implement, monitor, and maintain security policies and solutions to protect the Department's information assets. This position analyzes security risks, manages cybersecurity incidents, ensures compliance with security frameworks, conducts security assessments, and oversees security-related projects. This position works with Information Technology (IT) staff, management, and third-party vendors to maintain a robust cybersecurity posture for the Department. Perform related duties as assigned.

DISTINGUISHING CHARACTERISTICS

The information Security Analyst is a specialized classification within the IT series focusing on network and system security, incident response, and cybersecurity governance. The incumbent is expected to exercise sound and independent judgment in the performance of duties. The Information Security Analyst is distinguished from the Network and Systems Administrator by the former's primary focus on security controls, risk assessment, and compliance rather than general IT infrastructure management. This position reports to the IT Manager.

EXAMPLES OF DUTIES

The following duties are typical essential duties for positions in this classification. Any single position may not perform all of these duties and/or may perform similar related duties not listed here:

- Provide courteous and expeditious customer service to the general public and City and Department staff;
- Routinely adhere to and maintain a positive attitude toward City and Department goals;
- Conduct risk assessments and vulnerability analyses to identify security weaknesses;
- Monitor, analyze, and respond to cybersecurity threats and incidents;
- Manage cybersecurity-related policies, procedures, and best practices;
- Implement and manage security solutions, including firewalls, IDS/IPS, endpoint protection, and SIEM solutions;

- Perform regular security audits and compliance checks;
- Monitor network and system activity for security breaches or anomalies;
- Investigate security incidents and provide timely remediation;
- Develop, update and execute incident response plans and conduct cybersecurity drills;
- Work with IT staff to remediate vulnerabilities and prevent future incidents;
- Remediate vulnerabilities and mitigate the risk of security incidents. This entails direct responsibility for implementing fixes, patches, and configuration changes promptly, with appropriate testing and documentation;
- Ensure compliance with industry regulations and security frameworks (e.g., NIST, CIS, ISO 27001, CJIS, CCPA);
- Assist with security documentation, reporting, and audits;
- Manage identity and access control policies, including privileged access management;
- Conduct security awareness training for employees and IT staff;
- Develop guidelines and best practices for secure computing within the Department;
- Communicate emerging threats and recommend mitigation strategies;
- Secure systems and operational technology (OT) used for water distribution;
- Collaborate with relevant teams to Implement network segmentation and monitoring solutions for OT environments;
- Detect and mitigate threats targeting ICS infrastructure;
- Develop and enforce Zero Trust policies across all IT systems;
- Secure cloud-based workloads (e.g., Azure AD, Microsoft 365, AWS);
- Implement cloud access security brokers (CASB) to monitor SaaS applications;
- Implement Security Orchestration, Automation, and Response (SOAR) for automated threat mitigation;
- Use AI-driven anomaly detection to identify insider threats or compromised accounts;
- Automate log analysis and reporting;
- Work with other sections of the Department to optimize cyber insurance policies;
- Conduct cost-benefit analysis for new cybersecurity investments;
- Develop cyber risk quantification models to prioritize security spending;
- Assess vendors' cybersecurity postures prior to contract approval;
- Enforce vendor security policies for software and hardware providers;

- Implement Software Bill of Materials (SBOM) tracking to detect vulnerable software components;
- Collaborate with physical security teams to integrate cybersecurity with access control systems;
- Secure IoT devices such as smart meters and remote monitoring systems;
- Maintain security logs, reports, and documentation;
- Represent the Department in cybersecurity-related meetings and committees; and
- Perform other related duties as assigned.

QUALIFICATIONS

Any combination of education, training, and experience that would likely provide the knowledge, skills, and abilities to successfully perform in the position is qualifying. A typical combination includes:

Knowledge of:

- Cybersecurity principles, frameworks, and best practices;
- Network Security protocols, firewalls, IDS/IPS, VPNs, and endpoint security;
- OT and ICS security considerations;
- Security compliance frameworks such as NIST 800-53, CIS, ISO 27001, CJIS, and CCPA;
- Incident response methodologies and forensics analysis;
- Security Information and Event Management (SIEM) solutions;
- Zero Trust security models and cloud security controls.

Ability to:

- Conduct risk assessments of Department information technology infrastructure, systems, and devices and make recommendations for necessary changes;
- Respond to and investigate security threats, incidents, and violations;
- Troubleshoot, diagnose, analyze, and resolve information security problems and identify and recommend alternative solutions;
- Monitor information technology security vulnerabilities; implement approved measures to ensure integrity and security of infrastructure and systems;
- Work collaboratively with Department staff to identify and implement security solutions for business process improvements and efficiencies;
- Recommend and implement new, enhanced, or modified information technology security systems and tools;
- Prepare clear, concise, and accurate technical documentation, user guides, reports of work performed, and other written materials;

- Understand, interpret, and apply all pertinent laws, codes, regulations, policies, and procedures, and standards relevant to work performed;
- Integrate technology solutions across multiple platforms;
- Communicate complex technology issues clearly to non-technical parties;
- Maintain a variety of filing, record keeping, and tracking systems;
- Organize work, set priorities, meet critical deadlines and follow up on assignments;
- Effectively use computer systems and software applications relevant to work performed and modern business equipment to perform a variety of work tasks;
- Communicate clearly and concisely, both orally and in writing, using appropriate English grammar and syntax;
- Use tact, initiative, and judgment within general policy and procedural guidelines;
- Maintain a variety of filing, record keeping, and tracking systems;
- Remediate vulnerabilities and mitigate the risk of security incidents. This entails direct responsibility for implementing fixes, patches, and configuration changes promptly, with appropriate testing and documentation, as well as managing related assigned projects through to completion;
- Develop and implement cybersecurity governance frameworks and Department-wide security policies aligned with standards such as NIST, CIS, and ISO 27001;
- Quantify cyber risks using modeling and impact analysis to prioritize mitigation strategies and security investments;
- Design and manage automated incident response workflows using Security Orchestration, Automation, and Response (SOAR) platforms;
- Use AI-driven anomaly detection and behavior analytics to identify insider threat and compromised accounts;
- Configure, monitor, and tune SIEM solutions for proactive detection, alerting, and investigation of security events;
- Apply Zero Trust security principles to cloud and hybrid environments, enforcing least-privilege access and network segmentation;
- Secure Microsoft 365, Azure AD and SaaS environments using identity governance, multifactor authentication (MFA), and CASB tools;
- Implement Software Bill of Materials (SBOM) tracking and enforce vendor security compliance for software and hardware providers;
- Assess cybersecurity posture of third-party vendors and manage contractual enforcement of cybersecurity standards;
- Secure OT/IS systems used in water distribution through segmentation, protocol-aware detection, and secure remote access;

- Collaborative with operational and engineering staff to protect smart meters, IoT devices, and telemetry syetems;
- Deliver Department-wide security awareness training tailored to different roles and functions;
- Communicate emerging cybersecurity threats and strategies to management and cross-functional teams in a clear, actionable manner;
- Lead or participate in incident response drills, policy development committees, and cyber risk assessments;
- Draft, present, and maintain comprehensive cybersecurity documentation including policies, standards, and audit reports;
- Establish and maintain positive and effective working relationships with those contacted in the course of work;
- Maintain a driving record which meets Vehicle Code Standards and is acceptable to the Department and its insurance carrier.

MINIMUM QUALIFICATIONS

Education/Experience:

Bachelor's degree in Cybersecurity, Information Security, Computer Science, Information Technology, or a related field;

And

Three (3) years of progressively responsible experience in IT security, cybersecurity operations, network security, or a related field.

OR

Associate's degree in Cybersecurity, Computer Science, Information Technology, or a related field;

And

Five (5) years of progressively responsible experience in IT security, cybersecurity operations, network security, or a related field.

Desirable Certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- GIAC Security Essentials (GSEC)
- CompTIA Security+
- Microsoft Azure Security Engineer Associate

NECESSARY SPECIAL REQUIREMENTS

Possession of a valid Class “C” California driver’s license. For out of state applicants, a valid driver’s license is required and a valid Class “C” California driver’s license must be obtained within ten (10) days of appointment (CA Vehicle Code 12505c).

PHYSICAL TASKS AND ENVIRONMENTAL CONDITIONS

There is frequent need to stand, sit, stoop, walk, and perform other similar actions during the course of the workday. Employee accommodations for physical or mental disabilities will be considered on a case-by-case basis.

Must be able to see in the normal visual range with or without correction with vision sufficient to read small print, computer screens and other printed documents. Must be able to hear in the normal audio range with or without correction. Employee accommodations for physical or mental disabilities will be considered on a case-by-case basis.

Testing Standards: App Review/Supp App Review

Job Description:
BOWC Approved: 7/1/2025