CITY OF DALY CITY
JOB SPECIFICATION
EXEMPT

CYBERSECURITY ANALYST I-II

DEFINITION

Cybersecurity Analyst I: Under general supervision, provides professional level work, including the design, implementation, evaluation, and daily management of security systems and solutions; and performs duties related to threat detection and prevention, education, risk assessment, compliance, governance, business recovery, forensics, and incident response. This position requires a strong understanding of cybersecurity concepts, as well as the ability to work in a dynamic, public service-oriented environment. Other duties would include but not limited to assisting Network Administrators with items relating to the Network Administrator position.

Cybersecurity Analyst II: Under limited supervision, provides advanced level work, including the design, implementation, evaluation, and daily management of security systems and solutions; and performs duties related to threat detection and prevention, education, risk assessment, compliance, governance, business recovery, forensics, and incident response. This position requires a strong understanding of cybersecurity concepts, as well as the ability to work in a dynamic, public service-oriented environment. Other duties would include but not limited to aiding other Network Administrators with items relating to the Network Administrator position. Positions in this class require frequent use of a high degree of independent judgment and interpretative ability.

Positions in the Cybersecurity Analyst II classification are flexibly staffed and normally filled from advancement from the Cybersecurity Analyst I class, or when filled from the outside, require specific cybersecurity technology experience. Appointment to this class requires the employee to be performing substantially the full range of Cybersecurity Analyst II duties and to meet the qualifications for the class. The class requires the ability to work independently exercising judgment and initiative and a greater knowledge of the City's security systems and solutions.

EXAMPLES OF DUTIES

Architects, implements, monitors, maintains, and troubleshoots various security systems that protect the City's networks, IT/OT systems (including SCADA), applications and critical infrastructure; designs, organizes, modifies, installs, secures and supports security infrastructure; and provides technical support for network and security issues associated with enterprise applications; analyzes both raw and processed security alerts, logs and event data to identify potential security incidents, threats, mitigations, and vulnerabilities. Architects, implements, maintains, and troubleshoots the City's business continuity plan and emergency response plan as it relates to redundant, secure infrastructure. Investigates, analyzes, produces reports, and remediates security incidents that occur on

City systems and applications, both on-premises as well as in the cloud; confirms viable backups, test, maintains and monitors both on-premises and within the cloud; works closely with other government agencies, law enforcement, and external cybersecurity vendors to stay updated on emerging threats and response strategies. Performs other duties as required.

MINIMUM QUALIFICATIONS

Knowledge of: Network security, threat detection, and incident response; common cyberattack methods such as phishing, ransomware, and malware; security tools like firewalls, intrusion detection systems (IDS), and encryption technologies; government regulations, data protection laws, and compliance frameworks (e.g., PCI-DSS, CJIS, NIST, NERC CIP, ISO 27000, etc.) is essential, as is the ability disaster recovery planning and maintaining cybersecurity policies tailored to local government infrastructure is critical for ensuring the safety of sensitive public data and services.

Ability to: quickly respond to and mitigate cyber threats; analyze vulnerabilities specific to public sector environments. collaborate with internal teams and educating non-technical staff about security best practices; manage multiple tasks and prioritize threats is essential, as well as a keen attention to detail when conducting audits or reviewing security logs; adapt to evolving cyber threats and continuously update knowledge of emerging technologies and attack methods; think critically under pressure, especially during security breaches or system outages. interact positively and cooperate with co-workers, respond politely to customers, work as a team member, function under demanding time pressure, respond in a positive manner to supervision, and attend work and perform duties on a regular and consistent basis.

Experience:

Cybersecurity Analyst I: A minimum of 2-3 years of experience in cybersecurity or information security roles, preferably within government or public sector organizations.

Cybersecurity Analyst II: A minimum of 5 years of experience in cybersecurity or information security roles, preferably within government or public sector organizations.

Education:

Cybersecurity Analyst I: High school graduation or equivalent. Graduation from college or university with emphasis in computer science, information technology, or related field, and current certification (CCNA, MCSE, CCSA, CCSE, CEH, Security+) is desirable.

Cybersecurity Analyst II: High school graduation or equivalent. Graduation from college or university with emphasis in computer science, information technology, or related field, and current certification (CCNA, MCSE, CCSA, CCSE, CEH, Security+) is desirable.

License: Possession of a valid Class C California Driver License.

Applicants for this position must submit to a complete background investigation conducted by Daly City Police Department sworn personnel.

Rev: 08/2025