MAJOR FUNCTION

This is highly skilled work in the planning, implementation, monitoring and risk management of security measures to protect the City of Tallahassee computer systems, networks, and data from potential cyber threats and unauthorized access. Work is performed in accordance with industry best practices and security standards. An employee in this class is expected to exercise technical independence in implementing appropriate security controls, technologies, and risk management frameworks. Additionally, an employee is expected to safeguard the confidentiality, integrity, and availability of sensitive information through established processes & available technology. Work is performed under the general direction of higher-level supervisory staff who review the work through observation, conferences, reports, and by results obtained.

ESSENTIAL AND OTHER IMPORTANT JOB DUTIES

Essential Duties

Performs daily monitoring to detect and analyze threats and execute appropriate response procedures. Evaluates security requirements and design controls. Implements and operates security policies, procedures, and technologies such as Security Information and Event Management (SIEM), Endpoint Detection & Response (EDR), Governance Risk & Compliance (GRC), Data Loss Prevention (DLP), email security, and other access controls. Perform regular assessments to identify vulnerabilities and risks, analyze impact, and then recommend mitigation actions. Respond promptly to security incidents, investigating root causes, and implementing corrective measures to prevent recurrence. Safeguard the confidentiality, integrity, and availability of sensitive information through established processes & available technology. Performs related work as required.

Other Important Duties

Keeps abreast of the latest cyber threat intelligence, emerging cybersecurity technologies and/or frameworks. Performs related work as required.

DESIRABLE QUALIFICATIONS

Knowledge, Abilities and Skills

Considerable knowledge of cybersecurity policies, procedures, and technologies such as Security Information and Event Management (SIEM), Endpoint Detection & Response (EDR), Governance Risk & Compliance (GRC), Data Loss Prevention (DLP), email security, and other access controls. Knowledge of network devices uses and applications. Considerable knowledge of cybersecurity threats to include vulnerabilities, exploits, phishing, vishing, malware, ransomware, account takeover. Considerable knowledge of incident response and mitigation concepts such as containment and remediation. Understanding of relevant cybersecurity regulations, standards, legal requirements, secure network architecture and system design principles. Understanding of IT project management and/or project management institute concepts and processes. Key abilities include investigating and responding to cyber alerts/incidents, interpreting cyber threat intelligence, and implementing security policies & controls with strong analytical problem-solving, attention to detail, and documentation skills, along with the ability to stay current on emerging trends through research and continuous learning.

Minimum Training and Experience

Possession of a bachelor's degree; or possession of a high school diploma or an equivalent recognized certificate and three years of experience in an information technology, cybersecurity, or related customer service field.

Necessary Special Requirements

Must possess a valid Class E State driver's license at the time of appointment.

Must successfully complete a fingerprint-based criminal background screening and obtain the Criminal Justice Information Systems (CJIS) certification within 30 days of employment.

Established: 03-06-01
Revised: 04-23-04*
09-02-11*
01-26-15
06-28-24