IT SECURITY OFFICER

Department: Finance
Job Class #: 634900
Pay Range: Professional 18

FLSA: Exempt
Represented: No

Classification descriptions are intended to present a descriptive list of the range of duties performed by employees in this class and are not intended to reflect all duties performed within the job.

GENERAL FUNCTION: The Information Technology Security Officer under general direction, plans, directs and oversees the County's Information Security Program including technology, processes and practices to protect County technology and data assets from data security breaches and cyberattacks. Provides security focused leadership and best practices; establishes education and compliance programs; assesses security threats in relation to vulnerabilities; and develops incident response and mitigation plans. This is the top-level information security position reporting to the Assistant Director of Information Technology.

ESSENTIAL FUNCTIONS:
The following duties are a representative summary of the primary duties and responsibilities and are not intended to serve as a comprehensive list of all duties performed by all employees in this classification.

Strategy and Planning

- Forms a "center of excellence" for information security management, creates and maintains the IT security architecture design, and security standards policy, and promotes the advantages of managing information security risks more efficiently and effectively.
- Responsible for activities relating to contingency planning, business continuity management and IT disaster recovery in conjunction with 3rd parties (SAAS, PAAS).
- Leads information security risk assessments, oversees IT security audits and ensures timely response and remediation of audit findings.
- Keeps current with constantly evolving industry standards including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors.
- Serves as internal information security consultant; monitors advancements in cybersecurity technologies and advises senior management by identifying critical security issues; recommending risk-reduction solutions.

Acquisition and Deployment

- Recommends, selects and acquires additional security solutions or enhancements to existing security solutions to improve overall enterprise security as per the enterprise's existing procurement processes.
- Oversees the deployment, integration and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures.

Security Resource Management

- Leads the preparation and implementation of necessary information security policies, standards, procedures and guidelines, in conjunction with the IT Security Team committee.
- Responsible for county's cybersecurity program, including the technology and documented processes to ensure the county is secure from cyber-threats. Ensures third party testing is sufficient to evaluate effectiveness of the cybersecurity program.
- Achieves system security operational objectives by contributing information and recommendations for strategic plans; preparing and completing action plans; completing audits; identifying trends; determining system improvements; implementing change.
- Assists in the development and tracking of key performance indicators, balance scorecard, and other metrics for measuring operational outcomes of digital security initiatives.
- Produces both regularly reoccurring and targeted cyber threat intelligence briefings/products for consumption by both technical and senior leadership audiences.

- Supports malware and forensic analysis efforts in support of cybersecurity examinations, incident response and the overall strengthening of security posture.
- Maintains a high level of situational awareness in regards to emerging threats, threat actors and exploitation techniques.
- Works with technical teams and individuals to ensure the confidentiality, integrity and availability of the data residing on or transmitted to/from/through county workstations, servers and cloud systems.
- Partners with County experts (law enforcement, high-level leadership, etc.) in addressing threats to the County that include digital security.
- Accomplishes system security human resource objectives and supervisory responsibilities by recruiting, selecting, orienting, training, assigning, scheduling, coaching, counseling, and disciplining employees; communicating job expectations; planning, monitoring, appraising, and reviewing job contributions; planning and reviewing compensation actions; enforcing policies and procedures.
- Ensures compliance with relevant industry security standards including PCI for payment systems, PII for software systems, HIPAA for medical data, CJIS for law enforcement data; as well as other evolving standards.
- Advocates and recommends budget and resource requests to ensure compliance with the information security program.
- Actively participates in governance and oversight processes by providing information reporting and approved recommendations to Technology Investment Board (TIB) and IT Technology Committee (ITC).

Operations

- Leads, develops and implements cybersecurity and compliance monitoring technologies, processes, practices, policies, contracts, and 3rd party services to protect County business systems and data assets from service interruptions, damage, attack and unauthorized access. Maintains records of monitoring data, and documents any actions taken.
- Maintain effective communication with county departments and staff to facilitate and ensure adherence to policies and procedures.
- Supervise and coordinate activities of a designated unit; determine work procedures, prepare work schedules and determine methods for expediting workflow; assign, review and approve the work of subordinate staff.
- Ensure consistent interpretation of laws, rules, policies and procedures.
- Investigate grievances involving subordinates and recommend resolution; recommend hiring, promotional and disciplinary actions; approve leave requests, and overtime; assure adequate coverage during staff absences.
- Conduct performance evaluations and develop performance measures and standards.
- Develops and oversees a proactive, adaptive approach to information security threats. Performs risk assessments; develops response plans and mitigation plans in the event of a security breach. Serves as the Incident Commander if any security breach were to occur.
- Supervises the design and execution of vulnerability assessments, penetration tests and security audits as well as all investigations into problematic activity and provides on-going communication with senior management.
- Provides security review and subject matter expertise to ensure information security architecture and design considerations in major IT projects and programs. Participates in the evaluation of major hardware, middleware, application, and service selections.
- Reviews and advises on information security practices for vendors, service providers, operating partners, and any other entities managing data for, or on behalf of the County.

- Understands and manages the County's cybersecurity insurance and recovery resources and contracts.
- Performs regular security awareness training for all county employees to ensure consistently high levels of compliance with enterprise security documents.
- Ensures information security processes are documented, monitored and practiced by IT staff. Develops and maintains a central library of information security policies, standards and guidelines.
- Engages in ongoing communications with peers in the Systems and Networking groups as well as the various business groups to ensure enterprise wide understanding of security goals, to solicit feedback and to foster cooperation.
- Maintain regular, predictable and punctual attendance during regularly scheduled work hours at assigned worksite.
- Meet travel requirements of the position.
- Perform the physical requirements of the position; work within the established working conditions of the position.
- Work a flexible schedule, which may include evenings, weekends, and holidays.
- Lift and carry up to 25 lbs.

OTHER JOB FUNCTIONS:

- Perform other job functions as assigned.

SUPERVISION RECEIVED AND EXERCISED:

The IT Security Officer is a supervisory-level of the series with responsibility for cybersecurity of IT Operations. An employee in this class works under the general direction of the Assistant Director of Information Technology who observes work through assignments and projects to evaluate results achieved. This classification has full supervisory authority and is responsible to plan, assign, direct, supervise and evaluate the work of assigned staff.

WORK ENVIRONMENT: The work environment characteristics described herein are representative of those an employee encounters while performing the essential job functions. Work is performed in an office and IT equipment room environment. Work in construction areas to support IT needs for new and remodeled County office areas may be required. Work will involve traveling to various departments. Ability to work after normal County business hours, including weekends, for customer support, a scheduled function, or in an on-call capacity required.

PHYSICAL REQUIREMENTS: The physical demands described herein are representative of those that must be met by an employee to successfully perform the essential functions. Physical activities required are hand and finger dexterity necessary to operate equipment used in the position, talking, seeing and hearing. Walking, sitting, climbing and descending ladders, bending/stooping, working in and entering confined areas, pushing/pulling, and unassisted lifting associated with the job duties is required.

KNOWLEDGE, SKILLS, AND ABILITIES

Knowledge of:

- Principles and practices of effective supervision.
- Broad-based information technology and trends.
- Training techniques and skills to deliver effective training.
- Thorough understanding of a wide variety of Information Technology concepts and discipline areas.
- Integration between multiple computing platforms.

- Thorough understanding of ITIL concepts and terms.
- Thorough knowledge of County policies and business unit functions.
- Project management and team leadership.

Skill in:
- Use of independent judgment and effective decision-making in the application of a wide variety of laws, policies and procedures and in effective problem-solving.
- Leading and conducting all levels of project management.
- Information technology related problem resolution.
- Collaboration.
- Excellent customer service.

Ability to:
- Establish and maintain effective work relationships with elected officials, department heads, associates, and with the general public.
- Plan, assign and coordinate work.
- Understand and follow written and verbal instructions.
- Work effectively and productively with others.
- Communicate effectively verbally and in writing to audiences of various social, cultural, ethnic, educational and economic backgrounds.
- Effectively coordinate, perform and complete multiple duties and assignments concurrently and in a timely manner.
- Define, track, and assure responsiveness to clients' information technology problems.
- Motivate and lead others.
- Supervise teams, assign work, track time, evaluate work performance, and prepare status reports.
- Establish and maintain effective working relationships.
- Maintain regular, predictable and punctual attendance during regularly scheduled work hours at assigned worksite.
- Work a flexible schedule, which may include evenings, weekends, and holidays. May be subject to responding to emergency situations on twenty-four hour basis.
- Meet the travel requirements of the position.
- Physically perform the essential job functions of the classification.
- Categorize time spent, requests for service and assets according to provided definitions and help design structure for categorization for use by division

MINIMUM REQUIREMENTS TO APPLY:
- Bachelor’s degree in, information technology, computer sciences, business management information systems or closely related field and
- Seven or more years of information technology experience, including
- Three years of experience in an information security position and
- Two years in a project lead or supervisory role is required.
- An equivalent combination of experience and education which clearly indicates the ability to perform the essential functions of the position may substitute for the recruiting requirements on a year for year basis.

SPECIAL REQUIREMENTS AND/OR QUALIFICATIONS

- One or more of the following certifications (or other technology related credential and certifications) is desired:
    - CISSP Certified Information Systems Security Professional
    - CISM Certified Information Security Manager
    - GIAC Security Essentials Certification
    - GIAC Security Leadership Certification
    - ISACA Certified Information Security Manager

- A valid Washington State driver's license or the ability to otherwise meet the travel requirements of the position is required.
- Fingerprint and in-depth criminal history check are required.