IT Systems & Services Manager - Information Security Operations
Office of Technology & Information Services

BASIC FUNCTION

Under the direction of the Director of Infrastructure, the Manager of Information Security Operations manages the operations, activities, staff, and budget of the Security Operations division within the Office of Information Technology (OTIS); directs, oversees, monitors and evaluates the progress of the division toward meeting the department's roadmap of strategic goals, and defines, implements and modifies objectives, work plans, schedules, and commitment of resources to ensure that outcomes meet stakeholder needs and expectations with particular regard to Cyber Security, Information and Data security, and business continuity.

A leader for all security matters, including Governance, Risk, and Compliance, Cyber Security, Application Security, Identity and Access Management, Security Operations Management. Developing, implementing, and maintaining information security strategies, processes, training, guidelines, and projects to assure the confidentiality, integrity, and availability of District information systems, network, and data while complying with best practice frameworks and state and local regulations applicable to K-12 districts to move the District towards a more adaptive than reactive state.

REPRESENTATIVE DUTIES

The classification specification does not describe all duties performed by all incumbents within the class. This summary provides examples of typical tasks performed in this classification.

- Manage and oversee assigned staff of the designated division, Security Operations, within the Information Technology department in such areas as safeguarding our organization from intrusion, security threats, security weaknesses, software bugs and exploits, software and application development security validation,technical support including help desk, project management, infrastructure, enterprise solution management or similar.
- Oversee projects, coordinate resources and timelines and evaluate and approve activities and projects; monitor, support and manage assigned projects from implementation through completion to ensure specifications are met and assure appropriate equipment, materials, personnel and other resources are available to meet District technology needs; audit and asses solutions and outcomes and prepare a variety of narrative and statistical reports, records and files related to assigned activities including conclusions and operational recommendations.
- Ensure that projects are performed and completed within assigned budgets; authorize and control expenditures in accordance with established policies and procedures as appropriate; provide forecasting recommendations and input in the budget planning process.
- Oversee day-to-day operational activities in keeping with policies, procedures, and initiatives working to identify and safeguard the district from intrusion, security threats, security weaknesses, software bugs and exploits.

- Supervise and evaluate the performance of assigned staff, communicate job expectations, train, coach, counsel and discipline employees; interview and select employees and recommend transfers, reassignment, termination and disciplinary actions.
- Lead assigned staff and team members in identifying process improvement opportunities or strategies to achieve desired goals and objectives.
- Maintain and develop professional skills for self and employees through ongoing training and career development, including self-study, classroom training, and industry seminars and workshops; attend, participate in and lead meetings, conferences, seminars and trainings.
- Guide the development of security awareness and the security information continuity and disaster recovery plans.
- Oversight for incident-response, forensic IT audits, triage process, or related investigation. As necessary, lead the team, as the incident commander, in sharing knowledge with external entities including law enforcement, intelligence and other government organizations and agencies.
- Oversight for the execution of risk mitigation plans generated as a result of risk management analysis, penetration tests.
- Engage with external auditors, and other third parties in support of Security activities.
- Maintain an adversary understanding that drives a kill-chain activity based approach to detection, response, and recovery.
- Develop and manage cybersecurity Key Performance Indicators (KPIs)
- Ensure monitoring against authorized security control requirements and system risks, application configurations or vulnerabilities are reported.
- Lead the execution of security risk assessments for system, network, and software vulnerability, penetration testing, and manage related ongoing compliance monitoring activities, including project plans, estimations, specifications, flowcharts, and presentations.
- Collaborate and champion to department management, district leadership, staff and stakeholders to implement the policies, procedures, processes, controls, methods, best practices, and security awareness training needed to mitigate risk to information assets and ensure that mission-critical information resources are appropriately protected
- Manage the relationship between the Technical Support Representatives, Application Support, System Administration/Account Management, and Enterprise Solution Administration teams as it pertains to implementation and enforcement of internal controls, best practice, and overall District IT vision.
- Participate in the development and implementation of district wide strategic plans, policies, administrative directives, procedures and programs related to the delivery of technology and information services to users and set corresponding strategic direction and objectives for assigned division and staff as they relate to secure technical operations.
- Ensure all information technology systems, policies, directives, and procedures fully comply with applicable federal and state laws, standards, regulations (such as Data Protection Act, and ISO standards), and current District policies.
- Participate in strategic decision-making, system implementations, and the adoption and testing of new processes and procedures which improve the security and robustness of the organizational infrastructure and associated IT systems.
- Design, develop, and implement countermeasures, cyber security systems integration, and recommend tools to leverage specific to cyber security operations.
- Demonstrate a commitment to the Portland Public Schools Equity Initiative by developing a thorough knowledge and application of the district Racial Educational Equity Policy and other board policies; participate in staff development, in-services and trainings related to diversity, equity and inclusion in the

workplace and in K – 12 education; model appropriate behaviors; develop, recommend and implement improvements to educational business practices with awareness and understanding of their impact in a racially and culturally diverse community.

● Perform related duties as assigned.

DISTINGUISHING CHARACTERISTICS OF THE CLASS:

The Manager – Information Security Operations is part of the Information Technology Systems and Services Manager classification series.

This position calls for a high level of integrity, good judgment, knowledge concerning issues of privacy and confidentiality, excellent oral and written communication skills, ability to work as an independent, productive, responsible, self motivated member of a team in high pressure situations while maintaining a calm perspective.

EMPLOYMENT STANDARDS:

Knowledge of:
● Complex and advanced systems, processes and techniques in the assigned area of expertise.
● IT concepts, basic operating principles of computer hardware and software technical support functions; network, database and cloud-based technologies and related hardware and software applications.
● Operations, capabilities and limitations of computer equipment.
● Principles of effective supervision and training, planning, organization and project management.
● Technology and computer software related to business operations, data security, curriculum and instruction.
● Strategic planning, organization and project and workflow management techniques.
● District policies, procedures, and organizational structure.
● Applicable local, state and federal laws, codes, rules and regulations including FERPA, CIPA, and COPPA..
● Oral and written communication skills.
● Principles of employee management, development, motivation supervision and training.
● Principles of budget administration, public agency and purchasing principles, preparation and controls.
● Public education business processes and student information management programs, traditional and ERP software, systems and related applications.
● Interpersonal skills using tact, patience and courtesy; techniques and principles of high-quality customer service.
● Information security concepts, regulations, standards, and technologies
● Good understanding of current legislation and regulations pertaining to K-12
● Knowledge of relevant IT Security related hardware, software and vendor solutions

Ability to:
● Plan, organize, control and administer an assigned area of the District's information technology services, staff and activities.
● Assure efficient and timely delivery of program services, projects and activities.
● Communicate technical concepts and procedures to a variety of technical and non-technical audiences and serve as a technical resource for District personnel.

- Think strategically and develop short and long term technology plans, lead and participate in the development and implementation of, division policies and practices.
- Read, understand and provide detailed information concerning policies and procedures where judgment, knowledge and interpretation of procedures and regulations are required.
- Operate a variety of technologies and software.
- Maintain current knowledge of technological advances in the field.
- Advocate for best practices and state-of-the-art technologies.
- Monitor and control expenditures to ensure compliance with budget
- Conduct studies, analyze data and prepare, deliver and direct the preparation of a variety of public presentations, comprehensive narrative and statistical reports.
- Advocate, model, learn and implement Portland Public Schools Racial Equity Initiative.
- Educate, lead, promote and champion a culture that encourages and embraces diversity in the workplace.
- Establish and maintain collaborative working relationships across teams, functions and layers with district staff and external stakeholders.
- Supervise, plan, direct and evaluate the work of others.
- Deliver a high-level of customer service to district stakeholders.
- Analyze situations accurately and adopt an effective course of action.
- Maintain confidentiality and demonstrate discretion, initiative and good judgment.

Education and Training:
Is typically obtained through the completion of a Bachelor's degree in Engineering, Computer Science, Management Information Systems, Information Technology or other related area, including technical expertise in current hardware and software technologies.

Experience:
A minimum of five (5) years of experience working with information technology enterprise systems, software, communications, and network protocols, two (2) of which must include information security experience and three (3) of which must be at a supervisory level, overseeing technical programs and staff, functions and activities, developing and implementing budgets, operational policies and procedures within a large-scale, comprehensive information technology department, or one (1) year as a PPS IT Supervisor, is required.

Experience managing information technology professionals in a public agency and experience leading large, enterprise-level projects and information technology implementations are preferred.

Information security training and/or certifications such as security+, GSEC, CEH, CISSP, GIAC, or other security-related certifications are highly desirable.

Any other combination of education, training and experience which demonstrates the candidate is likely to possess the skill, knowledge, ability and trait characteristics essential for this classification may be considered. An Associate's degree in one of the identified disciplines and two (2) additional years of experience at the supervisory level may substitute for the Bachelor's degree requirement; a Master's degree in one of the identified disciplines may substitute for two years of the required experience.

Special Requirements:

Positions in this classification require the use of a personal automobile and possession of a valid driver's license.

WORKING CONDITIONS

The conditions herein are representative of those that must be met by an employee to successfully perform the essential functions of this job. Persons with certain disabilities may be capable of performing the essential duties of this class with or without reasonable accommodation, depending on the nature of the disability.

Work Environment: Work is performed primarily in a standard office environment with public contact and frequent interruptions.

Hazards: Potential conflict situations.

Physical Demands: Primary functions require sufficient physical ability and mobility to work in an office setting; dexterity of hands and fingers to operate a computer keyboard and other office equipment; sitting, standing and walking for extended periods of time; kneeling, bending at the waist; lifting, pushing, pulling and carrying office equipment, supplies and materials weighing up to 25 pounds; repetitive hand movement and fine coordination to use a computer keyboard; emotional stability to work effectively under pressure and to keep all aspects of the job under control; hearing and speaking to exchange information in person or on the telephone; seeing to read, prepare and assure the accuracy of documents.