City of Portland

CLASS SPECIFICATION

INFORMATION SECURITY MANAGER

[*CLASS CODE*]

[ESTABLISHED DATE]

CLASSIFICATION SUMMARY

Reports to a Director or Deputy Director within the Bureau of Technology Services (BTS). Under minimal direction, plans, manages, supervises, coordinates, and evaluates information security activities and operations. Classification is exempt from Civil Service.

Responsibilities include: managing the planning, implementation, monitoring, and reporting of information security within BTS; developing, monitoring, and exercising governing authority over Citywide information security policies and procedures; ensuring the confidentiality, integrity, and availability of all City data and communications systems and assets; developing and measuring compliance with information security policies and procedures; minimizing risk through implementation of effective technical, administrative and physical security controls; developing and maintaining BTS business continuity and a disaster recovery plan; managing the work of a team of security architects.

DISTINGUISHING CHARACTERISTICS

Information Security Manager is a single-incumbent and management-level classification.

Information Security Manager is distinguished from the Information Systems Manager series in that the former is responsible for ensuring Citywide information security and the latter is responsible for a broad range of information technology solutions.

Information Security Manager is distinguished from the Manager series in that the former exercises management responsibilities over an organizational unit responsible for information security and requires specialized education, knowledge, and/or training.

ESSENTIAL FUNCTIONS

The incumbent may perform a combination of some or all of the following duties, and perform related duties, as assigned.

General Duties:

1. Manage Citywide information security; assist in the development of strategies, policies, and initiatives to implement the strategic plan; provide financial administration; implement and administer policies, procedures, programs, goals, and objectives.
2. Coordinate with Bureaus/Offices, data custodians, and governance groups in the development, implementation, and monitoring of information security policies, standards, procedures, and security plans; oversee the dissemination of policies, standards, and procedures to Bureaus/Offices and other stakeholders; develop and measure compliance with information security policies and procedures.
3. Ensure information system and program security compliance with federal, state, local, and industry laws, regulations, rules, and policies.
4. Ensure the confidentiality, integrity, and availability of all City data and communications systems and assets; maintain network security and firewalls and intrusion protection devices; administer and coordinate work of external contractors and auditors to assess the efficacy of the City's

compliance efforts; manage and evaluate the design, development, acquisition, and implementation of information security infrastructure and solutions.

5. Develop and implement ongoing risk assessment program focusing on information security and privacy matters; recommend methods for vulnerability detection and remediation; oversee vulnerability scans and testing; minimize risk through implementation of effective technical, administrative and physical security controls.
6. Develop and maintain BTS business continuity and disaster recovery plan; support Citywide efforts to define and implement disaster recovery for key services, business processes, systems, and information; coordinate and participate in exercises to assess City execution of business continuity plans and disaster recovery efforts; develop an incident response plan and procedures.
7. Coordinate the development and delivery of a training and education program on information security and privacy matters for employees and other authorized users.
8. Manage the work of consultants including selection, negotiating terms and conditions, and authorizing work and payments; ensure all activities are consistent with City strategic direction and standards.
9. Assist in the preparation of strategic plans and lead the development of information security goals, objectives, policies, standards, priorities, and tactical work plans for the implementation of information security; develop, implement, improve, and evaluate programs, projects, workflow, methods, processes, systems, procedures, and work products in accordance with plans, budgets, and policies; perform specialized financial, revenue, budgetary, and management studies and analyses.
10. Participate in unit budget development and administration; forecast resources needed for staffing, equipment, materials, and supplies; manage unit and project budgets, including program, payroll, operating, and capital; monitor budget to actual revenues and expenditures and suggest mid-year or other adjustments; direct and oversee budget cost/benefit and resource requirement analyses.
11. Develop and establish performance requirements and personal development targets for staff; coach, train, and manage performance; monitor and provide coaching for improvement and development; evaluate performance and complete annual performance reviews.
12. Provide leadership to attract, develop, and retain diverse, highly competent, service-oriented staff that support the City's and Bureau's mission, objectives, and service expectations; create and promote an equitable workplace that demonstrates an environment respectful of living and working in a multicultural society; ensure that employees are provided with guidance and opportunity to correct deficiencies, and appropriate discipline procedures are implemented.

SUPERVISION RECEIVED AND EXERCISED

The work of this classification is performed under minimal direction by the BTS Director or Deputy Director.

Directly supervises Information Security Architects and other staff as assigned.

KNOWLEDGE/SKILLS/ABILITIES REQUIRED

1. Thorough knowledge of the principles and practices of leadership, operational and strategic planning, business communication, public administration, program evaluation, and budget preparation and administration.
2. Thorough knowledge of principles of management, supervision, training, and performance evaluation.
3. Thorough knowledge of relevant federal, state, and local laws, statutes, regulations, and ordinances and the ability to analyze, interpret, explain, and apply them.
4. Thorough knowledge of relevant security tools, such as identity management, access control, end-point protection, firewalls, IDS/IPS, security incident and event management (SIEM), vulnerability management tools, penetration testing tools, or web application firewalls.

5. Thorough knowledge of operating systems security frameworks.
6. Knowledge of project management methods, tools, and techniques, including project cost accounting, change management, and control.
7. Ability to manage functions and operations, including personnel management, budget administration, and apply program practices to diverse and complex City services.
8. Ability to communicate effectively, both verbally and in writing; present information, proposals, and recommendations clearly and persuasively in public settings; draft and review technical, policy and procedure, and audit documentation.
9. Ability to apply analytic and problem-solving skills to independently develop sound decisions, conclusions, and recommendations.
10. Ability to establish and maintain effective working relationships with those contacted in the course of work; demonstrate tact, diplomacy, and patience, and gain cooperation through discussion and collaboration.
11. Ability to manage a multicultural workforce, promote an equitable workplace environment, and apply equitable program practices to diverse and complex City services.
12. Ability to analyze Bureau/Office business, communication, and information technology needs, identify alternative technological approaches, and develop integrated, efficient, and cost-effective implementation plans.

MINIMUM QUALIFICATIONS REQUIRED

Any combination of education and experience that is equivalent to the following minimum qualifications is acceptable.

> **Education/Training**: Bachelor's degree from an accredited college or university with major course work in information technology, telecommunications, computer science, engineering, or related field;
>
> AND
>
> **Experience**: Eight (8) years of progressively responsible information technology management experience, including four (4) years in a supervisory role.

Special Requirements and/or Qualifications:

None.

Preferred Qualifications:

Experience working for a public agency in a supervisory or management role.

A professional certification or specialized training in information security.

Minimum Salary: xxxxx per [pay period, month, annual]
Maximum Salary: yyyyy per [pay period, month, annual]
Bargaining Unit: Non-represented
FLSA Status: Exempt
HISTORY
Revision Dates: