CITY OF PORTLAND **30002108**

INFORMATION SECURITY ARCHITECT

FLSA Status: Exempt
Union Representation: Professional and Technical Employees (PTE)

DEFINITION

Positions in this classification are responsible for contributing to the design of the City's software and infrastructure security architecture. Focus is on security design, policy recommendation, audit compliance and the development of guidelines for use by other Bureau of Technology Services (BTS) divisions in managing their operational security.

Information Security Architects research, analyze and document assigned security topics and provide recommendations to management for solutions, enhancements, and approaches. Incumbents develop access and audit controls, contribute to security strategies, and incorporate industry standards and best practices in support of the City's information security architecture. Positions at this level require significant independence in research and analysis and the ability to integrate thorough knowledge of all information system functions with information security expertise to develop solutions with broad scale impact.

EXAMPLES OF WORK:

(Any one position may not include all of the duties listed nor do the listed examples include all tasks which may be found in positions of this class.)

1. Contributes to the development of enterprise information security strategy and policies; collaborates with management to establish future direction for system security; surfaces potential policy changes from observed issues or problems; researches, designs and recommends strategies, approaches and options for assigned topics; evaluates security systems, tools or software and makes recommendations to management; conceives and designs approaches, methods and procedures for accomplishing security goals.

2. Contributes to the implementation of standards for assigned security topics; identifies, researches and analyzes industry and vendor standards and best practices; compares and consolidates multiple standards and recommends the elements that should apply to city operations - balancing security and business operational concerns; vets recommended standards with operational areas; reviews and comments on standards proposed by operational areas.

3. Develops and recommends guidelines and functional requirements for secure configuration and operation of the City's information assets; uses policies and standards to develop more detailed guidelines with specific examples and situations which will help operational security staff in

administering their systems; identifies low and high risk situations, types of file, etc; balances City operational requirements with appropriate security considerations; documents guidelines; assists other teams in understanding guidelines; explains standards and policies behind guidelines.

4. Consults on the development of new and changing information systems to ensure all security concerns, requirements and responsibilities are addressed; determines security requirements; evaluates business strategies and requirements; applies security standards; conducts system security and vulnerability analyses and risk assessments; identifies integration issues; develops and recommends access controls; prepares cost estimates; identifies security technology solutions for complex environments and architecture including cross-platform interoperability.

5. Audits security practices in BTS divisions; develops, recommends and implements appropriate audit processes and controls for assigned information security standards, functions or processes; ensures that regular monitoring and auditing occurs; reviews operational compliance with internal and external standards and policies; conducts or leads information security audits; documents and reports on results and recommendations.

6. Provides consultation and support to BTS divisions regarding operational security; provides advice and explanations; investigates security breaches.

7. Monitors new product developments and security trends; conducts research; makes recommendations regarding technologies which have the potential to benefit the security of information assets.

8. Evaluates security controls employed by cloud service providers and other third party providers; ensures information assets are adequately protected.

9. Leads security projects; clarifies project goals; gathers cross-functional team members; determines and manages timelines; performs and directs analyses and cost estimates; presents findings to management with recommendations.

KNOWLEDGE, SKILLS AND ABILITIES:

- Formal training or industry certification related to information technology security skills, such as: GIAC, CISSP, CISA, or Certificate of Cloud Security Knowledge (CCSK).
- Advanced knowledge of Payment Card Industry- Data Security Standard (PCI-DSS), HIPAA/HI-TECH Act, or Cloud Security Alliance.
- Advanced knowledge of one or more of the following security tools: 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.
- Advanced knowledge of one or more operating systems such as Windows, Unix/Linux, VMWare ESX, or Microsoft Hyper-V.

- Advanced knowledge of web application security.
- Advanced knowledge of the TCP/IP protocol and various common application protocols.
- Advanced knowledge of various directory services technologies, including Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory and Active Directory Federation Services (ADFS).
- Advanced knowledge of hardening standards, such as the associated Center for Internet Security (CIS) Security benchmarks and tools such as Microsoft Windows Group Policy.
- Advanced knowledge in drafting and reviewing technical and policy, procedure and audit documentation.
- Advanced knowledge of Software Development Life Cycle (SDLC) practices.
- Ability to lead a technical team on a complex project
- Ability to evaluate situations, recognize exposure and opportunity and make recommendations
- Ability to analyze and assess security needs, technology needs
- Ability to perform advanced technical analysis and design in support of citywide technical security structures
- Ability to assess and extrapolate implications of policy options
- Ability to develop conceptual models of security systems and their requirements and design security architecture
- Ability to develop clear and concise documentation and procedures and detailed guidelines for use by others
- Skill in analysis and assessment
- Skill in using logic to develop strategies
- Effective communication skills; ability to influence others, communicate clearly, and maintain effective working relationships

WORKING CONDITIONS

Physical Conditions: May require maintaining physical condition necessary for sitting for prolonged periods of time; extensive use of computer keyboard; extensive verbal and electronic communication with system users; near visual acuity for performing programming or software installation functions. Some positions require the ability to lift, carry and move computer equipment weighing up to 50 pounds.

License or Certificate

Industry certification related to information technology security skills, such as: GIAC, CISSP, CISA, or Certificate of Cloud Security Knowledge (CCSK) preferred.

Classification History:

Adopted: December 11, 2013
July 2017 – Updated union name from COPPEA to PTE