

JOB DESCRIPTION

Dept.: Information Technology

Working Title: Senior Information Security Analyst
(775)

Date: October 2018

Job Class: 15-12

PRIMARY FUNCTION:

The Senior Information Security Analyst is a senior position responsible for providing leadership, technical guidance, recommending and implementing security controls to safeguard KPU's valuable information assets. The analyst will also act as a liaison and work with all KPU business units as well as tactical hands-on resources in IT operations including incident detection and response. The position reports directly to the Director of Information Security.

JOB DUTIES AND TASKS:

Primary Duties

- Coordination and completion of information security operations documentation.
- Works with the Director of Information Security to develop strategies and plans to enforce security requirements and address identified risks.
- Coordinates the KPU Information Security Program deliverables.
- Reports to IT leadership concerning residual risk, vulnerabilities and other security exposures, including misuse of information assets and noncompliance.
- Plays an advisory role in application development or acquisition projects to assess security requirements and controls and to ensure that security controls are implemented as planned.
- Collaborates on critical IT projects to ensure that security issues are addressed throughout the project life cycle.
- Works with IT staff to identify, select and implement technical security controls.
- Researches, evaluates and recommends information-security-related hardware and software, including developing business cases for security investments.
- Scheduled reporting on Server and Desktop patch management compliance.
- Provide Information Security Awareness training and presentations to the KPU community.
- Coordinates the annual PCI DSS compliance requirements with IT and Finance.
- Monitors and reports on Information security feeds for new vulnerabilities.
- Establish unit goals and objectives and determine priorities.
- Monitor and assess project performance.
- Provide security technical advice and recommendations for system/network/telecommunication products and services

Vulnerability Management

- Manages all Internal and External annual vulnerability scan assessments
- Manages the approved KPU Security vendor partners.
- Coordinates all vulnerability mitigation activities resulting from the scan assessments.
- Provides full assessment reporting to the Director of Information Security.

Incident Detection and Response

- Provides third-level support and analysis during and after a security incident.
- Assists IT staff in the resolution of reported security incidents.
- Participates in security investigations and compliance reviews, as requested by internal or external auditors.
- Acts as a liaison between incident response leads and subject matter experts.
- Prepare Incident reports and present to the Director of Information Security.

Research, evaluate and plan

- Research Information Security technologies.
- Compile statistics/information and perform trend analysis for the various security systems.
- Research and evaluate technology to enhance system/network/telecommunication security.
- Leads in the design and planning of Information Security infrastructure.

Manage the acquisition and maintenance of KPU's Information Security hardware and software

- Maintain contact with information security technology service providers to keep apprised of developments.
- Recommend, monitor and evaluate supplier services.
- Oversee the receipt, inventory, testing maintenance and installation of Information Security equipment.

Audit and Risk Management Support

- Manages relationship with the KPU Organizational Risk department. Receives audit findings, and manages the collection of responses and remediation plans with owners.
- Works within the information security governance process to define control recommendations that are both efficient and effective.
- Provides oversight and management of audit finding remediation, including generating requirements for full remediation, providing feedback and suggestions on managerial responses to findings, and tracking progress and providing status and updates to the enterprise compliance team for reporting purposes.
- Supports e-discovery processes to include identification, collection, preservation and processing of relevant data.

SUPERVISION RECEIVED:

Reports to the Director of Information Security

SUPERVISION/DIRECTION EXERCISED:

Guide the information security awareness of new staff, co-op students. Provide Information Security Awareness training to users including faculty and employees.

PHYSICAL ASSETS/INFORMATION MANAGEMENT:

- Recommends information security best practices to the IT Leadership Team
- Handle confidential information in a responsible manner consistent with the Freedom of Information and Privacy Act.
- Understand and maintain confidentiality and is responsible for the appropriate use of privileged information and facilities access.

FINANCIAL RESOURCES:

- Participate in the preparation of cost estimates of information security hardware and software
- Provide input towards the purchase of software, related documentation and training materials.
- Verify receipt of purchase

The above statements reflect the general details considered necessary to describe and evaluate the principal functions of the job identified, and shall not be construed as a detailed description of all the work requirements that may be inherent in the job.

EMPLOYER REQUIRED KNOWLEDGE SKILLS AND ABILITIES:

- Completion of a college or university diploma/degree in computing studies supplemented by 5 + years' progressive experience in an Information Security related field with demonstrated experience related to IT security, auditing and compliance functions.
- Experience leading planning/implementation major IT projects
- Comprehensive general understanding of information risk concepts and principles, as a means of relating business needs to security controls.
- Understanding of key trends and players in the Information Security industry, particularly with respect to enterprise solutions, and cloud based technologies.
- Demonstrated knowledge of Operating System patch management tools
- Good understanding of Active Directory User and Group administration.
- Knowledge of the fundamentals of project management, and experience with creating and managing project plans, including budgeting and resource allocation.
- Good understanding of risk assessment methods and technologies.
- Some proficiency in performing risk, business impact, control and vulnerability assessments.
- Superior organizational skills with the ability to set priorities, follow-up and ability to manage multiple concurrent initiatives to meet challenging deadlines. Ability to research, evaluate and plan the implementation of emerging technology.
- Excellent technical knowledge of Microsoft Windows desktop and server operating systems and a wide range of security technologies, such as network security appliances, identity and access management (IAM) systems, anti-malware solutions, automated policy compliance tools, and desktop security tools.
- Excellent verbal and written communications skills and well developed interpersonal skills
- Ability to work under minimal supervision, under own initiative and as an effective team leader.
- Ability to independently organize work to achieve predetermined goals and meet deadlines.
- Knowledge in developing, documenting and maintaining information security policies, processes, procedures and standards.
- Knowledge of network infrastructure, including routers, switches, firewalls, and the associated network protocols and concepts.
- Strong analytical skills to analyze security requirements and relate them to appropriate security controls.
- Ability to interact with KPU's personnel at all levels and across all business units.
- Demonstrated leadership abilities, with the capability to develop and work within an information security team.
- A strong customer/client focus, with the ability to manage expectations appropriately, to provide a superior customer/client experience and build long-term relationships.

Knowledge Skills & Abilities revised:
