#### Trent University LogoOPSEU JOB DESCRIPTION

**Job Title:** Information Security Analyst

**Job Number:** C-082 | VIP: 1923

**Band:** OPSEU- 10

**Department:** Information Technology

**Supervisor Title:** Manager, Information Security

**Last Reviewed:**  June 27, 2023

#### **Job Purpose:**

Reporting to the Manager, Information Security, the Information Security Analyst is a subject matter expert in ensuring the security and continuity of existing and proposed technology infrastructure, systems, applications, and data access services. The primary mandate of the Security Analyst is to operate, institute and oversee information security systems and solutions to protect the confidentiality, integrity, and availability of IT assets and data university wide. The Security Analyst will assist in performing routine risk and vulnerability assessments, aid in establishing IT security controls and monitoring routines that align with industry best practices. The Security Analyst will also work closely with IT security partners, vendors and industry peers as information, service, and knowledge sources.

This position will work closely with the other IT units in implementing information security policies, standards, regulations, and guidelines to minimize IT security and compliance risk in the operation and use of IT systems and services, ensuring alignment with the business needs and the risk posture of the institution. This position will play a vital role in the development of end-user security education, awareness, and training campaigns to foster a culture of heightened awareness of risks and best practices across the institution. This position will work with, on a daily basis, highly confidential information.

#### Key Activities:

##### Security Operations

Risk Management/Vulnerability Management

* Identifies and implements scanning, patching, and penetration testing tools.
* Schedules regular scans of the institution’s systems to identify vulnerabilities.
* Works with groups inside IT to triage and track identified security problems.
* Under the guidance of the Manager, Information Security helps to implement procedures and processes to remove or mitigate vulnerabilities as they arise.
* Advises Manager, Information Security and IT management of potential risks and collaborates on strategies to mitigate those risks.
* Maintains an awareness of current IT security industry emerging vulnerabilities.

Security Controls

* Along with the Manager, Information Security, advises technical teams in the installation and use of information security software/components, such as firewalls, data encryption, anti-malware agents, access controls and analyst systems to protect the institution’s restricted and confidential data.
* Installs and manages measures to reduce the risk of the proliferation of malware or other IT security threats on end user systems including end-user system management.
* Installs and manages measures to protect university servers including patch management and ensuring up to date prevention and detection solutions are in place.
* Assists end-users with escalated cybersecurity questions including MFA issues, permissions and assists with providing users with best practice guidance.
* Performs operational administration, maintenance and troubleshooting of various security applications including end point security software, third party security systems/applications and cross-functional issues.

Monitoring

* Monitors the institution’s networks and systems for security breaches or intrusions daily including monitoring of the SIEM, XDR/EDR and Microsoft security tools.
* Monitors email gateways and responds to 'phishing' emails and 'pharming' activity.
* Assists with the planning and installation of upgrades, patches, performance, and usage issues on security systems.

Assessments

* Making recommendations to the Manager, Information Security, conducts information security assessments of new applications, providing guidance and insight into information security best practices and university workflows.

##### Support

Plans, Policies & Standards

* Documents critical processes including countermeasures or mitigating controls.
* Prepares technical documentation for IT security processes, procedures, and standards.

Education, Awareness & Communication

* Fosters education and awareness of IT information security throughout the university through the development of an IT security communications strategy
* Assists with the creation, maintenance, and delivery of cyber security awareness campaigns.
* Tests end users on their security awareness through simulated phishing.
* Builds awareness through IT security digital communications, website, posters, etc.
* Strives to develop a trusted communication and feedback loop with end users to ensure business needs are met and any risk responsibilities are understood.
* Conducts one on one and group training sessions as needed, including orientation sessions.
* Gives advice, guidance, and assistance to end-users on issues security related questions or issues such as spam and unwanted or malicious emails.
* Liaises with departments to improve security on a variety of business systems and applications, considering cross-functional processes, procedures, and standards.
* Presents technical security concepts, technologies and plans to institutional stakeholders as needed.

#### Education Required:

* General Degree (3 year) in Computer Science, Information Technology, Information Security or equivalent.
* A valid entry level Cybersecurity Practitioner Certification such as the Security+, SSCP or equivalent.

#### Experience/Qualifications Required:

* One (1) year of direct information security experience and five (5) years of total information technology experience.
* Experience managing cybersecurity systems including SIEM technologies, Microsoft Security (Azure AD, SSO, Defender for Endpoint).
* Fundamental understanding across the Information Security spectrum to include but not limited to: Firewall and Network Security, Security Architecture, Cloud Security & Network Defense.
* Experience introducing new security concepts, technologies, and processes to end-users.
* Experience conducting risk assessment reports of potential vendors following a prescribed assessment framework.
* Experience conducting risk assessments of information security threats and vulnerabilities as part of an overall incident management framework.
* Experience delivering information security information in a variety of formats including blog posts, social media, threat and technical briefing notes, website material and presentations.
* Understanding of information security assessment strategies and frameworks including NIST, PCI-DSS, ISO 27002 and COBIT.
* Experience working with the higher-education services landscape including partner organizations such as ORION, CANSSOC and the Canadian Center for Cybersecurity.
* Up-to-date knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors
* Knowledge of various security technologies e.g., single sign-on, application access control, identity management, digital signatures, audit, authentication techniques, monitoring, and network security
* The ability to communicate professionally, both oral and written to users of various backgrounds and levels of technical expertise including presentations to a wide audience
* Ability to analyze problem situations quickly and act to minimize service disruptions.
* Ability to understand the overall role of IT security in an educational setting and its impact on internal and external stakeholders.
* Strong analytic and investigative skills as well as strong technical report writing.
* Ability to analyze complex technical information to identify patterns and trends.
* Ability to work as part of a team and to build strong relationships with staff and other relevant individuals.

**Job Evaluation Factors:**

##### Responsibility for the Work of Others

* Consultation and infrequent direction of students and vendor providers who are contracted to work on specific projects.

##### Communication

Internal:

* University departments – Communication of information security efforts across all university departments.
* University employees – Distribution of training material, best practice coaching and cyber-security related advice.
* Students, Staff and Faculty – Assistance with the management and resolution of common cybersecurity issues.

External:

* Vendors – For the purpose of completing vendor risk assessment questionnaire.
* Colleagues at other institutions – participation in cybersecurity communities of practice at the appropriate level.