**Department of Human Resources**

**OPSEU Job Description**

**Job Title:** Level 1 Information Security Officer

**Job Number:** C-080

**NOC:** 2171

**Band:** 11

**Department:** Information Technology

**Supervisor Title:** Manager, Cybersecurity and Client Outreach

**Last Reviewed:** June 30, 2020

**Job Purpose**

This position is responsible for coordinating the confidentiality, integrity and availability of computer and information systems at Trent University. This highly motivated team player will work with minimal supervision to integrate and coordinate information security practices and processes throughout the IT department and Trent University as a whole.

This role will be responsible for the administration and monitoring of technical security safeguards and countermeasures including the university intrusion detection system, Palo Alto firewalls, patch and encryption management software and document security (RMS) system, as well as other information and network security technologies. In addition, this role will be instrumental to the implementation of new services and major changes to existing IT services, to ensure proper security compliance with regulatory, internal and external standards. This role will include extensive work architecting cyber security and computer systems, project management and emergency (crisis) management.

Finally, this role will work directly with key stakeholders across the university to implement and develop cyber security related policies and best practices and direct the work of other IT units in cyber security efforts. This role will have a heavy focus on user education and training, as well as support and coaching to assist with the development of “security as a practice” process models. This role will be required to work on a daily basis with highly confidential material.

**Key Activities**

* Provide cyber security leadership, technical expertise and advice to the following groups:
	+ Information Technology service desk staff – For assisting with responding to the day to day cyber security needs of the institution.
	+ Information Technology system administrators and programmers – To assist with security design and implementation relative to new and existing IT services and processes.
	+ Information Technology Management Team – For the development of internal processes, standards and policies related to the cyber security needs of the institution.
	+ Employees and managers of other university departments – In order to assist with the development of workflows and processes that conform to information security guidelines and best practices.
* Under the supervision of the Manager, Cybersecurity and Client Outreach, design and develop information security policies, best practice guidelines and workflows to ensure regulatory and standards compliance with NIST, ISO, PCI, PIPEDA and other relevant frameworks, standards and legislation.
* Maintain up-to-date knowledge of cyber security trends and events and contribute to communities of practice in the cyber security industry by participating in special interest groups, attending conferences related to cyber security and conducting research into cyber security trends.
* Regularly conduct penetration tests of university computer systems, disaster recovery and other simulated emergency exercises to assess overall readiness.
* Develop and maintain IT disaster recovery, business continuity and emergency operations plans to integrate with the overall university risk management practices.
* Conduct risk analysis of external vendors, internal processes and departmental practices to assess operational cyber security risk.
* Regularly perform audits and of internal processes, departments, vendors and processes to ensure compliance with relevant standards such as the NIST framework.
* Administer the university intrusion detection system and SIEM systems - construction of customized scripts in relevant IDS systems such as Snort, Bro, and FortiSIEM to deliver a highly focused security management platform to the university IT department.
* Assist with the architecture of and coordinate the use of Microsoft management technologies to deliver optimized information security policies to desktop and remote users – including, but not limited to, Active Directory management and architecture, Group Policy, Azure Active Directory and MFA, MBAM and System Center..
* Coordinate the functionality of a centralized patch management and endpoint security management system.
* Coordinate the delivery of user awareness campaigns and training related to information security for students, staff and faculty at the university.
* Providing end user support, training and consultation regarding the best practice for security operational issues.
* Maintenance of an awareness of industry best practices; liaise with vendors and other third party providers to stay abreast of technology evolution, software revisions, bug fixes, and to obtain product information.
* Act as the primary point of contact for any information security issues, and manage security related events in accordance with internal policies and established best practices.
* Receiving and managing confidential, personal, and proprietary information using sound judgment to remain in compliance with all university policies and privacy legislation applicable to the situation.

**Education**

* 4-year degree in a computer technology related discipline – Computer Science, Computer Information Systems, Computer Engineering or equivalent of extensive technology focused education and other related discipline.
* Valid information security focused certification from International Information System Security Certification Consortium (ISC)2

**Experience Required**

* 5+ Years of experience working in an information technology field with at least 2 years of combined focus on cyber security related activities (training, administration or management)
* Experience in the delivery of training seminars and conference presentations with 1-2 years’ experience in the delivery of security related awareness training and assessment.
* Extensive experience with risk management and policy development principals, security frameworks and standards including NIST, PCI and ISO.
* Experience working in the educational industry with directly relatable knowledge on the operation of higher education.
* Extensive experience implementing information security focused training and awareness in both a technical and non-technical context.
* Experience working with a number of network security technologies including Intrusion detection systems, firewalls, ACLs, patch management systems.
* Experience working with Microsoft network technologies including Active Directory, Group Policy and System Center.
* Strong analytical and problem solving skills.
* Excellent communication (oral, written, presentation), interpersonal and consultative skills.

**Responsibility for the Work of Others**

This role will be responsible guiding information security best practice internally to the IT department and externally for other university departments. As such, this role will be required to work with relevant managers to ensure that security related tasks are accomplished.

**Communication**

Internal:

* University departments – Coordination of information security efforts across all university departments.
* University managers and senior executives – management reports and briefings
* University employees – Distribution of training material, best practice coaching and cyber-security related advice.

External:

* Vendors and potential vendors – for the purposes of implementation of new solutions
* Colleagues at other institutions – participation in the CUCCIO Information Security Special Interest Group as designated representative for Trent University.
* Public groups – Information security focused industry groups, contacts and conferences.