Nipissing University
JOB DESCRIPTION

JOB TITLE:	Security Analyst
DEPARTMENT:	University Technology Services (UTS)
CLASSIFICATION:	Technologist F
WAGE GRADE:	110
EMPLOYMENT STATUS:	Full-time Support
SUPERVISOR:	Manager, Infrastructure Support

SUMMARY OF FUNCTIONS:

Reporting to the Manager, Infrastructure Support, the 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. Providing support to the Security Architect, the primary mandate of the Security Analyst is to recommend, institute and oversee approved 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 University IT security partners, vendors and industry peers as information, service and knowledge sources.

This position will work closely with the Security Architect and the UTS management team in establishing and assessing 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 holds a critical role in all incident response management situations and activities which may be sensitive in nature and involve restricted and confidential data. Professionalism and confidentiality are essential in this position.

DUTIES & RESPONSIBILITIES:

OPERATIONS (80%)

Risk Management/Vulnerability Management

- Identifies and implements scanning and penetration testing tools
- Schedules regular scans of the institution’s systems to identify vulnerabilities
- Under the guidance of the Security Architect, helps to implement procedures and processes to remove or mitigate vulnerabilities as they arise
- Advises Security Architect and UTS 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 Security Architect, 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

- Develops measures to reduce the risk of the proliferation of malware or other IT security threats on end user systems including end-user system management
- Develops measures to protect university servers including patch management and ensuring up to date prevention and detection solutions are in place
- Performs operational administration, maintenance and troubleshooting of various security applications including end point security software, third party security systems/applications and cross-functional issues
- Makes recommendations for security controls and best practice features within specific enterprise wide software solutions

Monitoring

- Monitors the institution's networks and systems for security breaches or intrusions on a daily basis
- Monitors the SIEM and security systems for alerts and anomalies
- Liaises with external managed SOC (Security Operations Centre)
- Recommends, acquires and oversees the installation of intrusion detection and monitoring software
- Monitors email gateways and responds to 'phishing' emails and 'pharming' activity.
- Upgrades, patches, performance and usage issues on security systems

Assessments

- Considers data security in all aspects of UTS operations, identifying issues and recommending solutions to UTS management on improvements to the confidentiality, integrity and accessibility of institutional data
- Advises on the selection and implementation of new systems or solutions including risk assessments, Privacy Impact Assessments (PIA) and SOC (system and organization controls) report analysis
- Conducts security assessments, including testing of processes, system and application vulnerability testing and risk assessments

Incident Management

- Works as an integral part of the incident response team in the case of an IT security incident or related outage
- Follows established UTS procedures and protocols for incident response, recommending updates or changes post incident
- Aids in technical and forensic investigation into any breaches, reviewing extent of any damage
- Documents incident activities in real time using established tools and procedures
- Assists the Security Architect in preparing reports of findings and recommendations to management

Support **(20%)**

Plans, Policies and Standards

- Works with the Security Architect and UTS management to develop a set of security standards and best practices for the institution, recommending security enhancements to stakeholders based on these
- Assists the Security Architect and UTS management with the continual maintenance of the Nipissing University IT security incident response plan
- Assists the Security Architect in the development and maintenance of an IT Security Strategy
- Documents critical processes including countermeasures or mitigating controls
- Prepares technical documentation for IT security processes, procedures and standards

Education, Awareness and 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, creating NU metrics (e.g. simulated phishing tests)
- 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 employees 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

Other duties as assigned

QUALIFICATIONS:

Education: Bachelor degree in Computer Science, or equivalent

Training and/or experience may be substituted for formal academic training at the discretion of the university.

Training, Experience, Knowledge & Skills Required:

- Three to five yeas of relevant experience
- Must be bondable and receive a negative Criminal Record Check
- A certificate in one of the following would be considered an asset
  - Certified Information Systems Security Professional (CISSP)
  - Certified Information Security Manager (CISM)
  - Certified in Risk and Information Systems Control (CRISC)
  - Certified IT Architect Foundation (CITA)
  - Information Technology Infrastructure Library (ITIL)
  - Control Objectives for Information and Related Technologies (COBIT)
- Experience in areas of technical training and development; project management; vendor/product evaluation, selection, and implementation; tactical planning
- Project management skills and/or exposure to project-based work structures
- Expertise across the Information Security spectrum to include but not limited to: Firewall and Network Security, Security Architecture, Cloud Security & Network Defense
- Experience in the introduction of new security technologies into various levels of an organization
- Knowledge of forensic and incident management techniques; basic understanding of compliance and regulatory issues
- Experience with hosted and cloud services, especially IaaS, SaaS and PaaS, and the related security implications and control approaches
- Experience working with a SIEM (Security Event Monitoring)
- Experience with endpoint management solutions, firewall management, intrusion prevention detection solutions (IDP)
- Experience with Linux and Microsoft server administration, networking technologies as well active directory/LDAP
- Understanding of PCI and other IT security standards
- Ability to consistently categorize, measure, and prioritize security risks, express them in the language of the business unit to make them easily digestible by system owners and assist in their mitigation
- Knowledge of FIPPA, ISO 27002, PCI and the Ontario government information security policy
- High level of personal integrity, as well as the ability to professionally handle confidential/sensitive matters, and show an appropriate level of judgment and discretion
- Ability to work independently with minimum direction and can manage own workload/commitment, including the ability to prioritize tasks and problem solve in a high-pressure environment
- Knowledge of vulnerability assessment tools and processes
- Knowledge of security attack pathologies and risk assessment procedures

- 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 in order to identify patterns and trends
- Ability to work as part of a team and to build strong relationships with staff and other relevant individuals

POSITION / CONTACTS:

Supervised by: Manager, Infrastructure Support

Interpersonal contacts: Students, faculty and staff

External contacts:

- Board members
- Security Services
- Other universities and colleges
- Peers in SIGs and industry
- Judicial bodies
- Vendors and contractors
- Architects, engineering, consultants, construction contractors
- Government agencies
- Policy/security agencies
- Prospective students, parents, alumni

MATERIALS UTILIZED:

- General office and computer equipment and systems
- Security tools, logs and reports
- Technical manuals and related online resources
- Policy and procedures manual and related online resources
- Security related internet resources

PHYSICAL/MENTAL DEMANDS & WORKING CONDITIONS:

- Periods of intense mental concentration and moderate physical demands during incidents and outages
- Periods of high stress during incidents and outages
- Visual, mental and listening concentration
- Frequent interruptions, conflicting demands
- Available to respond 24/7 to incident and outage situations
- Flexible work schedule is required (evening and weekend work may be required)
- Comfortable working environment
- Occasional travel
- Occasional overtime during incidents and outages

I have read my position description and it has been reviewed with my supervisor. I understand what my duties and functions are, and I will carry out all of my responsibilities as herein described.

____
Employee Name (please print)

____ ____
Employee Signature Date

Approvals

____ ____
Supervisor Date

____ ____
Assistant VP, Human Resources & Equity, Diversity & Inclusion Date