

Nipissing University
POSITION DESCRIPTION

POSITION TITLE:	Manager, IT Security and Emerging Technologies
DEPARTMENT:	University Technology Services (UTS)
SALARY LEVEL:	SL 7
EMPLOYMENT DEFINITION:	Full-time Administration
SUPERVISOR:	Director, Technology Services
DATE POSITION CREATED:	August 2026

SUMMARY OF FUNCTIONS:

Reporting to the Director, Technology Services, the Manager, IT Security and Emerging Technologies provides day-to-day management, security oversight and continuous improvement for assigned cybersecurity, information security, artificial intelligence and intelligent automation services. The Manager leads assigned security and AI/automation functions, supervises technical staff, supports operational planning and ensures related reviews, assessments and response activities are completed effectively and consistently.

The Manager provides operational leadership for cybersecurity and the responsible adoption of artificial intelligence, automation and digital innovation, by supporting the implementation of approved policies, standards, governance requirements and risk controls across assigned services and initiatives. The position identifies and assesses risks, recommends mitigation measures to the Director, Technology Services, and oversees approved implementation within the authority of the position.

As a member of the UTS management team, the Manager contributes subject-matter expertise to operational and strategic planning, supports institution-wide technology initiatives, and works with academic and administrative partners to translate approved University priorities into secure, practical and sustainable technology solutions. Overall institutional technology strategy, enterprise risk acceptance, final policy approval and priority-setting across the full UTS portfolio remain with the Director, Technology Services and the appropriate University authorities.

DUTIES AND RESPONSIBILITIES:

Security Operations, Governance and Cybersecurity

40%

- Manage and direct assigned information security and cybersecurity operations, including network, system, application, identity, access and data security activities, in alignment with approved UTS priorities and University requirements
- Lead the development, implementation and maintenance of operational security standards, procedures, guidelines, controls and documentation within assigned areas
- Lead and ensure completion of security risk assessments, third-party security reviews and impact assessments for systems, services, vendors and digital initiatives
- Oversee cybersecurity incident response activities, including investigation, analysis, containment, remediation, documentation, post-incident review and follow-up action tracking, in coordination with the Director and the UTS management team and in accordance with the University's Incident Response Plan
- Provide advice and recommendations to the Director, UTS managers and partners on cybersecurity posture, emerging threats, vulnerabilities and practical risk mitigation options
- Ensure that identified security risks, required corrective actions and compliance obligations are documented, assigned, tracked, escalated and followed through in a consistent and auditable manner

- Contribute to the development, testing and maintenance of contingency, disaster recovery and operational resilience practices related to information systems and data
- Maintain current knowledge of privacy, data protection, freedom of information, cybersecurity and other relevant legislative, regulatory, contractual and sector requirements, and coordinate related operational compliance activities
- Escalate significant institutional risks, resource requirements, policy decisions and risk-acceptance matters to the Director, Technology Services

Emerging Technologies and Responsible Technology Adoption

30%

- Manage and support the responsible assessment and implementation of approved artificial intelligence, automation and other emerging technology initiatives within UTS and in collaboration with academic and administrative areas
- Develop and maintain operational processes, guidelines, review practices, documentation and controls that support the responsible, transparent and appropriate use of emerging technologies
- Work collaboratively with University partners to identify and assess opportunities for emerging technologies to support employees in their work, improve service quality, enhance access to information and strengthen the sustainability of University operations
- Lead operational assessments of proposed initiatives, considering privacy, security, ethics, accessibility, policy, data, procurement, service delivery and potential impacts on University processes and employees, and escalate significant institutional risks or decisions to the Director
- Coordinate implementation activities for approved initiatives, including requirements gathering, consultation with affected areas, documentation, testing, training, change support and operational handoff
- Support meaningful consultation and clear communication with affected areas and employees when emerging technologies may result in significant changes to established work processes or service delivery
- Promote appropriate human oversight, professional judgment and accountability in the assessment and implementation of technology-enabled processes
- Monitor developments in artificial intelligence, automation and other emerging technologies, vendor capabilities and higher-education sector practices, and provide recommendations regarding potential benefits, limitations, risks and operational considerations
- Provide practical guidance, awareness and learning opportunities to help faculty and staff understand and use approved technologies responsibly and effectively
- Establish and monitor appropriate measures to evaluate adoption, service quality, accessibility, operational effectiveness, risk and user experience associated with implemented initiatives
- Support institutional capacity through documentation, training, knowledge sharing and the development of internal expertise related to emerging technologies

Staff and Operational Management

15%

- Provide direct supervision, coaching, task assignment, performance management and professional development for the IT Security team and the Application Developer/Analyst
- Plan, prioritize and direct team activities, projects, service requests, workloads and operational follow-up to support reliable and responsive service delivery
- Foster a collaborative, inclusive, service-oriented and continuous-improvement culture within the team
- Manage assigned budgets, resource allocation, procurement activities and vendor relationships related to security, AI and intelligent automation services within approved authority
- Optimize the use of human, fiscal and technical resources by identifying priorities, dependencies, capacity requirements and operational risks
- Ensure team members maintain current technical skills, operational documentation and appropriate cross-training to support continuity and succession planning
- Participate in recruitment, selection, orientation and onboarding for positions within assigned areas
- Provide operational support or coverage for other members of the UTS management team, as assigned

Operational Planning, Service Improvement and Collaboration

15%

- Participate as a member of the UTS management team, contributing to operational planning, service alignment, project coordination and continuous improvement
- Collaborate with other UTS managers to support integrated, effective and secure service delivery across UTS
- Contribute subject-matter expertise, options and recommendations to UTS strategic and operational planning while working within approved University and departmental direction
- Develop short, medium and long-term operational plans for assigned services and projects, including priorities, resource requirements, dependencies, risks and implementation considerations
- Provide information and forecasts to support annual budget planning and lifecycle planning for security, AI and intelligent automation services
- Prepare recommendations, briefing notes, documentation, metrics and options analysis related to cybersecurity, AI adoption, intelligent automation, digital risk and emerging technology initiatives
- Participate in institutional committees, advisory bodies, sector forums and working groups as assigned or approved by the Director
- Build productive relationships with academic and administrative areas, vendors, and sector peers to support operational delivery and continuous improvement

Any other duties as assigned.

QUALIFICATIONS:

Education: University degree in Computer Science, Information Technology, Information Security or a related discipline.

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

Training, Experience, Knowledge & Skills Required:

- Minimum of five (5) years of progressive experience in information security, cybersecurity, enterprise technology, or related area, with exposure to artificial intelligence, intelligent automation or emerging technology initiatives, including demonstrated supervisory or team leadership experience
- Experience supervising technical or professional staff, assigning and prioritizing work, supporting professional development and managing performance
- Experience with security operations, security governance, risk assessments, incident response, third-party security reviews, vulnerability management, documentation and compliance-related activities
- Experience evaluating, implementing or operationalizing AI, intelligent automation or emerging technology solutions in a complex organizational environment
- Experience managing projects, vendors, procurements, operational budgets and competing priorities with finite resources
- Experience developing and implementing operational plans, standards, procedures, guidelines, controls and governance-supporting documentation
- Strong knowledge of cybersecurity principles, risk management, incident response, identity and access management, monitoring, application security, data security and network security
- Knowledge of privacy, access to information, data protection, accessibility, regulatory compliance and institutional policy considerations relevant to security, AI and intelligent automation
- Knowledge of AI and automation technologies, including associated risks and responsible-use considerations in institutional contexts
- Ability to exercise independent judgment and make operational decisions within approved policies, budgets, procedures and governance frameworks, while recognizing matters requiring escalation
- Ability to translate complex technical, security and AI concepts into practical guidance for non-technical audiences

- Strong leadership, communication, analytical, problem-solving, facilitation, documentation, presentation, organizational and time-management skills with the ability to support constructive resolution of issues
- Ability to develop effective relationships and work collaboratively with faculty, staff, students, administrators, vendors and external partners
- Ability to manage urgent issues, confidential information, significant operational risk and multiple priorities in a complex and evolving environment
- Must be bondable and receive a negative Criminal Record Check

RELATIONSHIPS/CONTACTS:

Supervised by: Director, Technology Services

Positions supervised:

- IT Security Architect (1)
- IT Security Analyst (1)
- Application Developer/Analyst (1)

Internal Contacts: Students, staff, faculty

External Contacts:

- Universities and colleges
- Sector associations, special interest groups and working groups
- Vendors, contractors and consultants
- Government, regulatory, privacy and security agencies
- Cybersecurity, AI, intelligent automation and technology partners
- Prospective students, parents, alumni

MATERIALS UTILIZED:

- Nipissing University strategic, academic and operational plans
- UTS strategic and operational plans
- University policies, procedures, standards and guidelines
- Applicable legislation, regulations, contractual requirements and sector frameworks
- Cybersecurity, AI, intelligent automation, monitoring, documentation, reporting and project-management tools
- Various software applications, computer systems and general office equipment

PHYSICAL/MENTAL DEMANDS & WORKING CONDITIONS:

- Participate in after-hours and emergency operational support, including response to cybersecurity incidents, urgent operational issues and emerging technology risks, in coordination with the UTS management team
 - High degree of mental concentration, analytical focus and attention to detail
 - Manage multiple priorities, urgent operational issues, cybersecurity incidents, frequent interruptions and shifting demands
 - Frequent handling of confidential, sensitive, technical, privacy, security and risk-related information
 - Requirement for sound judgment, diplomacy, discretion and timely decision-making
 - Majority of time spent in normal office conditions
 - Occasional travel and attendance at sector meetings or events
-

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

Human Resources

Date