*Algoma University is committed to undoing systemic and institutional discrimination and being publicly transparent and accountable. Diversity, equity, and inclusion are fundamental to our Special Mission. In keeping with the Seven Grandfather teachings that are the core values that inform our decisions as an institution, we are committed to creating a welcoming, inclusive, respectful, and safe environment where everyone belongs. We live these values through the strength and richness that diversity brings to our workforce and welcome contributors from equity-deserving groups including: Indigenous Peoples, Black and racialized persons, women, Persons with Disabilities, 2 Spirit, Lesbian, Gay, Bisexual, Transgender, and Queer persons.*

| | |
|---|---|
| **Job Title:** | **Director, Cybersecurity, Innovation & Technology**<br>*Administration* |
| **Position Status:** | Permanent, Full-time<br>*Non-Union* |
| **Department:** | Innovation & Technology (IT) |
| **Supervision Received:** | President & Vice-Chancellor |
| **Supervision Exercised:** | Manager, IT Projects and Development<br>Manager, IT Security and Networks<br>Manager, IT Service Operations |
| **Location:** | Sault Ste. Marie, ON or Brampton, ON |
| **Number of Positions:** | 1 |

## PRIMARY FUNCTIONS:

| | | |
|---|---|---|
| A. | Cybersecurity Leadership & Risk Management | 40% |
| B. | Enterprise Architecture, IT Strategy & Digital Transformation | 30% |
| C. | IT Infrastructure, Operations & Service Delivery | 20% |
| D. | Other Duties | 10% |
| **TOTAL** | | **100%** |

Algoma University has an existing vacancy in the position of Director, Cybersecurity, Innovation & Technology. Reporting to the President & Vice-Chancellor, the Director, Cybersecurity, Innovation & Technology is responsible for defining, implementing, and

overseeing Algoma University's cybersecurity strategy, IT architecture, and related practices. The incumbent is responsible for collaborating with the IT Team, a broad range of staff, and third-party vendors to effectively translate risk management strategies, tactics, and business objectives into specific security controls and architectural designs enabled by modern technologies and services.

## RESPONSIBILITIES:

### A. Cybersecurity Leadership & Risk Management (40%)

- Establish and maintain an institutional cybersecurity governance framework, ensuring clear accountability between IT, academic, and administrative areas.
- Regularly brief the President and Senior Executive on cybersecurity risk posture, compliance status, and emerging institutional risks.
- Oversee the development and maintenance of the university's cybersecurity risk register, presenting risk posture, mitigation strategies, and compliance metrics to senior leadership.
- Develop, maintain and monitor security policies, standards, and procedures to ensure compliance with relevant regulations and industry best practices.
- Develop a security architecture that balances risks and costs, serving as a roadmap for continually improving the security posture.
- Lead the ongoing security awareness training and education programs for faculty, staff, and students.
- Lead the creation and ongoing enhancement of a comprehensive institutional information security program that is aligned with industry best practices and relevant regulatory requirements, ensuring the university's data and systems are adequately protected.
- Lead regular risk assessments and implement appropriate security controls to mitigate identified risks.
- Develop and maintain incident response plans and lead response efforts in the event of a security breach or disruption.
- Stay abreast of emerging security threats and vulnerabilities and proactively implement countermeasures.
- Lead the integration of cybersecurity into business continuity and disaster recovery strategies to ensure resilience across IT infrastructure and critical systems.
- Oversee the design, implementation, and testing of robust security solutions in collaboration with IT teams.

- Evaluate and recommend security technologies and services to enhance the university's security posture.
- Oversee third-party and cloud security assessments, ensuring vendor risk management and mitigation plans are in place.
- Sponsor penetration testing, vulnerability assessments, and cybersecurity audits, ensuring timely remediation and institutional reporting.
- Collaborate with project teams to provide subject matter expert guidance and ensure that security is integrated at every stage of system development and deployment.

**B. Enterprise Architecture, IT Strategy & Digital Transformation (30%)**

- Develop and maintain the university's multi-year IT and digital strategy, ensuring alignment with academic, research, and institutional priorities.
- Provide leadership in defining and advancing the university's enterprise architecture and digital transformation agenda.
- Define, document, and implement IT architectural standards and strategic roadmaps that support the university's operational needs and long-term strategic goals.
- Lead the development and maintenance of an enterprise architecture framework that aligns with the university's strategic vision and goals.
- Lead the definition of data, cloud, and digital transformation strategies, embedding principles of privacy, security, and accessibility across initiatives.
- Provide leadership oversight of major IT projects and systems development portfolios, ensuring strong business cases, value delivery, and resource prioritization.
- Evaluate and approve technology investment proposals, ensuring lifecycle sustainability, cost-effectiveness, and institutional benefit.
- Build and maintain strong partnerships with academic and administration leaders to identify opportunities for innovation, process automation, and modernization.
- Foster collaboration and alignment across academic and university divisions to support effective change management and successful adoption of digital initiatives.
- Lead the assessment of current architectures and identify areas for improvement.
- Collaborate with users to gather requirements and translate them into architectural designs.

**C. IT Infrastructure, Operations & Service Delivery (20%)**

- Guide the design, implementation and oversight of IT systems and infrastructure to ensure scalability, interoperability, and security.

- Provide strategic direction and oversight for infrastructure, networks, cloud environments, and end-user support to ensure reliable, secure, and efficient service delivery.
- Define and monitor service-level objectives (SLOs) and key performance indicators (KPIs) to evaluate operational effectiveness and client satisfaction.
- Provide leadership and direction to IT managers, setting performance expectations, evaluating outcomes, and fostering a culture of accountability and service excellence.
- Support managers in vendor and contract management, ensuring compliance with institutional standards and value for investment.
- Lead integration and continuous improvement initiatives across service delivery, development, and security functions to ensure a cohesive, resilient, and efficient IT ecosystem.
- Develop, monitor, and deliver on cybersecurity and IT management KPIs to drive continuous improvement through data-driven insights.

**D. Other Duties (10%)**

- Other duties, as assigned.

## MINIMUM QUALIFICATIONS

- Undergraduate degree in Computer Science, Cybersecurity, Information Security, or a related field and a minimum of ten (10) years of progressive experience in cybersecurity and information technology, or an equivalent combination of education and experience, is required.
- Proven experience in leading enterprise-level IT operations, security or infrastructure and demonstrated leadership and strategic planning skills in complex IT environments, collaboration skills to drive digital transformation and change management initiatives.
- Proven ability to adapt strategies and operations in response to evolving cybersecurity threats and organizational priorities.
- Understanding of cybersecurity tools such as IDS/IPS, FW, MFA, SIEM, MDM, DLP, 802.1x, and PIA.
- Ability to collaborate internally and externally with peers and groups such as CUCCIO, OUCCIO, ORION ON-CHEC, CCCS (Canadian Cyber Security Centre) and others.
- Demonstrated ability to develop and implement cybersecurity policies and procedures aligned with organizational objectives and compliance requirements.
- Demonstrated business acumen with the ability to align cybersecurity strategies and initiatives with organizational goals, priorities, and risk tolerance.

- In-depth knowledge of security frameworks (e.g., NIST, ISO 27001), risk management methodologies, and security technologies.
- Strong understanding of enterprise architecture principles and frameworks (e.g., TOGAF, Zachman).
- Experience with cloud security and architecture is considered an asset.
- Professional security certifications (e.g., CISSP, CISM, CISA) are considered an asset.

**Salary Scale:** **$118,576 to $148,219 annually**

**To apply for this position please submit a resume and cover letter HERE.**

Algoma University is strongly committed to fostering diversity and inclusivity within our community and is an equal-opportunity employer. The university invites and encourages applications from all qualified individuals who would contribute to the further diversification of our Institution, including equity-deserving groups that are traditionally underrepresented in employment (Indigenous peoples, racialized persons, women, persons with disabilities, and 2SLGBTQQIPA+ persons).

In accordance with the Accessibility for Ontarians with Disabilities Act, 2005, upon request, accommodation will be provided by Algoma University throughout the recruitment, selection, and/or assessment process to applicants with disabilities.