Indigenous.Link

Canada's fastest growing Indigenous career portal, Careers.Indigenous.Link is pleased to introduce a new approach to job searching for Indigenous Job Seekers of Canada. Careers.Indigenous.Link brings simplicity, value, and functionality to the world of Canadian online job boards.

Through our partnership with Indigenous.Links Diversity Recruitment Program, we post jobs for Canada's largest corporations and government departments. With our vertical job search engine technology, Indigenous Job Seekers can search thousands of Indigenous-specific jobs in just about every industry, city, province and postal code.

Careers.Indigenous.Link offers the hottest job listings from some of the nation's top employers, and we will continue to add services and enhance functionality ensuring a more effective job search. For example, during a search, job seekers have the ability to roll over any job listing and read a brief description of the position to determine if the job is exactly what they're searching for. This practical feature allows job seekers to only research jobs relevant to their search. By including elements like this, Careers.Indigenous.Link can help reduce the time it takes to find and apply for the best, available jobs.

The team behind Indigenous.Link is dedicated to connecting Indigenous Peoples of Canada with great jobs along with the most time and cost-effective, career-advancing resources. It is our mission to develop and maintain a website where people can go to work!

Contact us to find out more about how to become a Site Sponsor.

Corporate Headquarters:
Toll Free Phone: (866) 225-9067
Toll Free Fax: (877) 825-7564
L9 P23 R4074 HWY 596 - Box 109
Keewatin, ON P0X 1C0

RESEARCH & IT SECURITY INTEGRATION ANALYST

Job ID	**42989-8633**
Web Address	https://careers.indigenous.link/viewjob?jobname=42989-8633
Company	McMaster University
Location	Hamilton, ON
Date Posted	From: 2022-01-24 To: 2050-01-01
Job	Type: Full-time Category: Education

Description

At McMaster University, our people are our most valuable asset. We strive to attract, develop, and retain talented faculty and staff, and to foster inclusive excellence which values the strengths, perspectives, and contributions of each individual. McMaster’s profile and stature has evolved to one of the Top 70 Universities in the World and we are recognized as Canada’s Most Research Intensive University. McMaster is also recognized as one of the top employers in the Hamilton/Niagara region and has been recognized as one of Canada’s Top Diversity employers in each of 2019, 2020 and 2021.Duties/Responsibilities and Qualifications:Our University Technology Services team mission is to provide exceptional customer service and a high level of support to the McMaster community. Our goal is to ensure transparency, innovation and accountability in service delivery and support. We stand by and value integrity, mutual respect, collaboration and cooperation in support of the University’s IT Strategic Vision of a connected One IT community.   McMaster Information Technology Security Services is a dedicated team of information security professionals focused on strengthening the IT Security posture of the Institution through education, process and standards and technological controls. The IT Security Services team delivers on day to day operational and service requirements as well as undertaking the necessary projects and implementation activities related to the IT Security Road map, a multi-year plan that includes a series of initiatives intended to strengthen the security posture of the Institution. A key component of the IT Security Roadmap is an information security plan focused specifically on supporting researchers and their research. This approach has been developed to address the growing focus and heightened attention on protecting researcher’s data and intellectual property from threat actors with specific attention to data management and compute and technology environments and infrastructure. Under the direction of the Senior Manager, Cyber Security Systems, in collaboration with McMaster Research Data Management (RDM) Services (co-managed by RHPCS and the University Library), the Research Security Integration Analyst provides a collaborative and engaging approach to support researchers and their research teams with IT security supports and services that will strengthen the overall IT security posture of research at McMaster. This role will also be responsible for advancing the Information Security priorities identified in the McMaster RDM Institutional Strategy and Security Plan for Researchers focused on information security awareness and training, supporting researchers and their teams in implementing information security services and supports such as Multi-Factor Authentication, End

Point Security tools; providing security guidance and advice to support researchers and their teams as they include information security requirements in research grant proposals; providing information security guidance advice and support as they set up and make changes to their computing environment in their labs and research technologies; provide support to researchers and their research teams as potential and confirmed security issues and events arise. The incumbent will be working directly with researchers; in many cases they will need to work with IT support units across campus, and specifically in the Faculties, that manage the existing systems and infrastructure used by researchers across related disciplines. For systems that are managed by a Faculty IT unit or RHPCS, for example, the engagement should be with members of those groups, as they'll understand the complexities of the systems, as well as the often unique requirements of the researchers and the complexities of working with them.The Research Security Integration Analyst acts as a lead technical and consulting resource to various University departments and units with respect to the planning, implementation, and maintenance of information technology systems. Supports the University's academic and administration departments by acting in a functional capacity in all phases of the Project Life Cycle for medium to large projects, including post-production support and ongoing maintenance. Continuously gains an understanding of the University's operations and processes and how systems are used in support of those operations. Creates, maintains, and manages multi-user, production quality campus-wide computing environments that involve computers, servers and associated hardware, software and facilities. Facilitates the selection of new information processing, computing technologies, information security and services across the University. Provides expertise in leading and participating in the technical architecture planning and acquisition of development projects and the documentation, final preparation, and introduction of new systems and services into the production environment. Provides lead-hand supervision to a team of Systems Administrators.

- Manage work assignments of internal staff and schedule and monitor adherence to procedures, protocols, and standards.
- Act as an on-site project manager, responsible for managing projects from inception to completion.

- Plan and establish project framework and identify project milestones to ensure the project is completed according to project specifications and within specified timelines.
- Design, develop, implement, and evaluate functional specifications for a variety of highly complex University application systems.
- Complete feasibility studies and cost-benefit analyses and translate technical flow into business terms.
- Coach and mentor junior staff in order to ensure a highly motivated and technically competent team.
- Participate in the development of capital project charters and cost justifications.
- Lead the ongoing design and support for technology in server and related environments, data network infrastructure and related environments, datacenter technology and facilities, storage area network and other storage related environments, voice network infrastructure and related environments, and information security infrastructure and other related environments.
- Critically evaluate information gathered from multiple sources, reconcile conflicts, decompose high-level information into details, abstract up from low-level information to a general understanding, and distinguish user requests from the underlying true needs.

- Elicit requirements using interviews, document analysis, requirement workshops, surveys, site visits, business process descriptions, use cases, scenarios, business analysis, and task and workflow analysis.
- Perform advanced levels of analysis, problem solving and research skills to formulate solutions to complex business needs.
- Conduct gap analyses.
- Develop strategies for implementing new services and upgrades on production systems.
- Troubleshoot computer system issues that may require an end-to-end evaluation of University wide systems often spanning multiple heterogeneous hosts and locations across the University and with external service providers.
- Ensure the availability and performance of the current production storage, information processing, and computing environment in assigned and related areas of the organization.
- Test system architecture in order to minimize risks to the production systems.
- Investigate, evaluate, compare, and demonstrate new hardware and software products, and new computing techniques which could enhance the University’s computing, information processing, and network environment.
- Undertake study and pilot projects to assess and select commercial technology alternatives.
- Provide technical assistance to individual user groups, user support, and operational staff in the introduction and development of specialized systems and services.
- Ensure individuals conform to organizational information processing, use of network, and computing standards through the proper publication and awareness of policies.
- Plan and coordinate the technology refresh for large and complex interconnected systems.
- Contribute to the development of cost and time estimates for the technical architecture components of project implementation.
- Deliver workshops and demonstrate new technologies to campus staff as systems are being implemented.
- Prepare and present training for user support and operational staff through technical seminars and documentation.
- Prepare procedures for restoring systems to full operation after hardware and software component failures on both production and test systems.
- Prepare contingency plans for recovering services and operations after incidents including, but not limited to, power blackouts, water damage, or structural building failures and contribute to the planning and development of disaster recovery scenarios.
- Undertake projects such as performance monitoring and capacity planning to monitor the overall reliability and effectiveness of the computing systems and information processing architecture including storage area networks.
- Liaise with computer vendors, other institutions, and associated computer user groups as a means to maintain communication between all parties involved in technical projects and day-to-day operations.
- Design, implement, and document support processes, procedures, and mechanisms that inter-connect heterogeneous systems in support of the integration of processes and data flow.
- Gather and compile information and create reports and graphs for capacity planning, and performance metrics.
- Prepare technical specifications and requests for quotes from suppliers and requests for proposals.

- Participate in negotiations with suppliers to discover options and acquire the most cost effective solutions for technology requirements.
- Utilize the appropriate control tools to coordinate projects according to Project Management Office methodologies.
- Develop success criteria and risk assessments for projects and changes.
- Develop, implement, and document best practices to align with departmental and University strategies and processes.
- Work independently with users to define concepts.
- Ensure that projects meet specified functionality requirements.
- Prepare and review recommendations and other project initiation documents.
- Document system functionality, particularly related to new enhancements.
- Develop and maintain information technology process flow, methodology, and control documentation.
- Assist with the development of project proposals and estimates.
- Resolve problems in the test, production implementation, and post-implementation phases in coordination with other technical and business groups.
- Liaise between the technology and support teams.
- Communicate project, issue, and system status to others.
- Communicate testing results to other stakeholders.
- Facilitate effective dialog between user community and technical staff.
- Interact with and exchange information with colleagues.
- Follow a test script and document defects.
- Prioritize and schedule issues resolution.
- Plan, schedule, and monitor own work within short time horizons.
- Organize individual time, work and resources to accomplish objectives in the most effective and efficient way.
- Understand and use appropriate methods, tools, and applications to complete work tasks.
- Demonstrate a rational and organized approach to work and identify development opportunities.
- Absorb technical information when it is presented systematically and apply it effectively.
- Use measurement methods to monitor progress toward goal attainment, tenaciously working to meet or exceed those goals, while deriving satisfaction from the process of goal achievement and continuous improvement.
- Ensure that the internal and external customer perspective is a driving force behind decisions and activities.
- Follow service practices that meet customers’ and University needs.
- Interact with others in a way that gives them confidence in one’s intentions and those of the University.
- Work collaboratively with others to achieve departmental and institutional goals. Actively participate as a member of a team to move the team toward the completion of goals.
- Perform a range of varied work activities in a variety of structured environments.
- Successfully engage in multiple initiatives simultaneously.
- Apply and enforce department change control policies and procedures.
- Read and understand a complex project plan and develop simple project plans.

- Remain current with relevant development and project methodologies.
- Remain current with security policies and procedures and work with System Administrators to implement security changes.
- Remain current with the different levels of testing and develop simple use cases and test scripts.
- Provide lead hand supervision and is responsible for the quality and quantity of work of others.
- Bachelor's degree in Computer Science, Business, or a related field of study.
- Requires 5 years of relevant experience.
- The incumbent must have demonstrated experience (5 plus years) and success with the following technologies, techniques, and principles:
- Working with end users, in particular Researchers and / or experience conducting primary research, to provide support for the use and adoption of technologies and troubleshooting issues such as:
- Multifactor Authentication
- Authenticating in a Microsoft environment
- Installation of security protection tools such as anti-virus, end point protection, malware detection

- Developing and delivering targeted and contextualized (in a research environment) Information Security training and awareness sessions such as:
- Phishing
- End Point Protection
- Email Protections including Multifactor Authentication
- Techniques and approaches to protect data
- Identification and response to Information Security incidents and events

- Building, managing and maturing End Point and Network security for hybrid environments that could be set up for research labs and research environments, including:
- Architecture, both current and future state
- Technologies, Tools and Systems, both physical and virtual
- Policies, Standards, Guidelines
- Processes and Protocols
- Security software, hardware and controls, including:
- End Point protection techniques
- Networking techniques
- TCP/IP (versions 4 and 6), DNS, DHCP, HTTP(S), SSH, etc.
- Virtualization
- Segmentation
- Administration Rights and Privileges Management
- Palo Alto Intrusion Prevention System
- Cortex end point protection
- Trend Micro Anti-virus
- Server and Operating system technologies, including:
- Linux, Windows, Active Directory, VMWare
- Microsoft, Azure
- Web application technologies, including:

- Apache, IIS, CMS/LMS
- Vulnerability Management technologies and principles, including:
- Tenable vulnerability scanning, Web Application Scanning, Common Vulnerabilities Enumeration, OWASP, penetration testing techniques
- Identity and Access Management technologies and principles, including:
- SAML, OpenLDAP, Active Directory

Relevant technology certifications are desirable. The incumbent must have the following:
- Demonstrated oral and written communication skills, in particular working with Researchers and / or in Research environments and working with a number of IT support units that manage the existing systems and infrastructure.
- Strong and creative problem-solving through engagement skills with Researchers and or in a Research environment that is supported by IT units that manage various aspects of their systems and infrastructure.
- Able to build high levels of trust the credibility across a diverse community of stakeholders, in particular Researchers, in order to impact and influence decisions and direction
- Collaborative, supportive, and energetic team player
- 3-5 years of experience within an information security role; relevant certifications are desirable
- Awareness of risk management principles and practices; relevant certifications are desirable
- Awareness of privacy principles and practices; relevant certifications are desirable
- Experience delivering effective, high quality Information Technology services and solutions
Relevant certifications are desirable.

For more information, visit McMaster University for RESEARCH & IT SECURITY INTEGRATION ANALYST