Reporting to the **Manager, Information Security**, the **Senior Cybersecurity Analyst** is responsible for information technology risk assessments, defining security architecture principles, and related activities in support of Sunnybrook’s Cybersecurity Program.

**Summary of Duties:**

**Design and Develop Security Architecture Principles:**

* Create and maintain security architecture frameworks and models for Infrastructure, Applications and Cloud Services.
* Define Cybersecurity requirements for projects as part of project design and implementation phase.
* Design security solutions that align with business requirements and objectives.
* Develop and implement security policies, standards, and guidelines along with any reference architecture materials.
* Collaborate with other key stakeholders such as IT Operations, Research and Architectural Standards Review Board (ASRB) to have the controls frameworks approved.

**Cybersecurity Risk Assessments**

* Conduct Threat Modeling activities to define use cases during a Risk Assessment.
* Establish the scope of the system or process being analyzed, including interfaces and data flows.
* Identify possible threats using various techniques, such as brainstorming sessions, checklists, and threat libraries (e.g., STRIDE, ATT&CK framework).
* Undertake technical security threat and risk assessments (TRAs) in accordance with industry-recognized standards, including the identification of administrative, procedural and technical control remediation items as required.
* Collaborate with other business units to identify security risks within their respective operational areas, make recommendations for appropriate security control remediation items and support the development of security process control improvements within those portfolios suitable for risk mitigation.
* Provide input for applying security controls based on Industry standards such as NIST CSF, ISO27001 or Cloud Security Alliance (CSA);
* Support project managers and teams in executing key security projects.
* Review IT security controls and processes for new services to ensure proper technical security controls are applied to systems and applications.
* Work with external consultants and third-party service providers as appropriate for independent security audits, incident response and risk remediation.

**Qualifications/Skills:**

* University Degree in Business Administration, Information Technology, or Engineering or equivalent. Master’s degree preferred.
* Minimum 5 - 7 years of experience in the role of Cybersecurity, Security Architecture or Security Operations.
* Understanding of key technology capabilities such as Network (e.g. Router, switch and VLAN security; wireless security), API’s, Cloud Services, Endpoint Detection & Response (EDR), identity and access management and other industry leading technologies.
* Understanding of Windows, UNIX and Linux operating systems VB.NET, Java/J2EE, ColdFusion, API/web services, scripting languages and a relational database management system (RDBMS) such as MS SQL Server or Oracle
* Strong understanding of Risk Assessment Methodologies and Approaches.
* Excellent communication skills; strong critical thing, analytical and negotiation skills
* Demonstrated knowledge of and/or familiarity with standards and frameworks such as NIST CSF, ISO/IEC 27000 series, SABSA or Cloud Security Frameworks.
* Demonstrated experience in undertaking supervised security threat and risk assessments, using an industry-recognized framework equivalent to the Harmonized Threat and Risk Assessment (HTRA) methodology.
* Certification in one or more IT governance or control standards such as SABSA, Microsoft Tools, ISC2 (e.g. CISSP), SANS, ISACA (e.g. CISM, CISA), PMI (e.g. PMBOK) or equivalent preferred.
* Knowledge of information technology project management, technology (software or hardware) development and/or technology operations management preferred.