#### Trent University LogoEXEMPT JOB DESCRIPTION

**Job Title:** Director, Information Security

**Job Number:** X-445| VIP: 1906

**Band:** EXEMPT-9

**Department:** Information Technology

**Supervisor Title:** AVP, Information Technology

**Last Reviewed:**  April 22, 2024

#### **Job Purpose:**

As the Director of Information Security, your mission is to safeguard the integrity, confidentiality, and availability of our critical information assets and systems. By developing and executing comprehensive information security strategies, policies, and procedures, you will ensure the protection of sensitive data, research findings, and intellectual property while fostering a culture of security awareness and compliance across all university stakeholders. Your leadership will be instrumental in proactively identifying and mitigating security risks, managing security incidents, and maintaining regulatory compliance to uphold the reputation and trust of our institution in the academic community and beyond. Through collaboration with cross-functional teams, you will champion innovative approaches to address evolving cyber threats and promote a resilient and secure information environment conducive to the pursuit of academic excellence, research innovation, and student success.

#### Key Activities:

* Develop and implement organization-wide information security strategy aligned with business objectives and best practices.
* Identify, assess, and prioritize security risks to information systems, data, and infrastructure.
* Establish and enforce information security policies, standards, and procedures for regulatory compliance and data protection.
* Conduct security awareness training programs for employees on policies, procedures, and best practices.
* Develop and maintain incident response plans for addressing security breaches and leading investigations.
* Design and implement security architectures to protect against cyber threats and ensure information integrity and availability.
* Evaluate and manage security risks associated with third-party vendors, ensuring contractual compliance.
* Oversee security audits and compliance initiatives to meet regulatory requirements and industry standards.
* Implement and manage security monitoring tools to detect and respond to incidents in real-time.
* Provide leadership and guidance on security governance, advising senior management and participating in committees.
* Prepare and present reports on security posture and compliance to senior management.
* Collaborate with stakeholders during security incidents to mitigate impacts and ensure compliance.
* Represent the university in information security-focused groups and drive continuous improvement initiatives.
* Provide leadership in IT vision and strategic direction, overseeing function-specific strategies and initiatives.
* Ensure information sharing and integration of university computing systems.
* Monitor plans, targets, and measures for reporting areas, and negotiate resources for projects.
* Lead the development of innovative business solutions to build organizational capabilities.
* Develop policies, standards, and controls for operational efficiency, compliance, and risk mitigation.
* Address functional challenges impacting the university community and develop working relationships with stakeholders.
* Act as the university’s representative to regional and national agencies and organizations.
* Oversees and ensures that all human resource practices and processes are complied with and develops leadership strength in functional areas by coaching reporting leaders and staff in the development of critical competencies and by modelling valued leadership behaviours.
* Provides career planning advice to staff and creates development plans to help staff achieve their career goals including assigning work which leverages their skills and capabilities and provides them with opportunities for learning.
* Directs the preparation, control, and administration of budgets for reporting areas and approves major expenditures.
* Negotiate and manage service-level agreements internally and externally.
* Maintain professional designations and stay updated on current IT techniques.
* Perform other related duties as required.

#### Education Required:

* Master’s degree required.
* Honours Bachelor’s Degree in Business Administration, Engineering, Computer Science, or related area from a recognized University with Canadian accreditation.

#### Experience/Qualifications Required:

* Over eight (8) years of progressive IT leadership experience in higher education or similar complex organizations.
* Proven experience in leadership or management within information security, preferably in large organizations or educational institutions.
* Ability to develop and implement comprehensive information security strategies aligned with organizational goals.
* In-depth understanding of regulatory requirements and compliance standards relevant to the education sector.
* Industry-recognized certifications such as CISSP, CISM, CISA, demonstrating expertise in information security.
* Excellent communication skills to convey complex security concepts to non-technical stakeholders.
* Strong analytical skills for risk assessment and developing mitigation strategies.
* Commitment to continuous learning and staying updated on emerging threats and best practices.
* Upholding high ethical standards, integrity, and professionalism in information security management.

##### Technical:

* Experience in leading diverse teams of security professionals and strategic planning.
* Proficiency in network security, application security, cloud security, identity and access management, cryptography, and security operations.
* Development and execution of incident response plans, including coordination with stakeholders.
* Collaboration with cross-functional teams, senior leadership, academic faculty, and external partners to promote security awareness.
* Conducting security risk assessments, threat modelling, and vulnerability management activities.
* Adaptability to evolving security landscape and technologies, driving innovation in security solutions.
* Promotion of a culture of ethics, accountability, and transparency within the organization.

##### Competencies:

* Customer Service: Leads customer-centric IT strategies, excels in stakeholder engagement and communication, exceeds service benchmarks, minimizes disruptions, and fosters innovation.
* Collaboration: Improves communication, shares credit, monitors and enhances team effectiveness, influences team strategy positively, and demonstrates commitment under challenging situations.
* Communicating for Results: Engages with leaders, seeks consensus, debates opinions, resolves conflicts, explains complex situations, and solicits expert perspectives for decision-making.
* Problem-Solving: Anticipates risks, forecasts trends, defines innovative solutions, and gains senior leadership approval for critical issues.
* Leading Self: Manages emotions, reflects on setbacks, seeks feedback, adapts to change, and positively influences others.
* Leading Others: Supports learning and development, mentors talent, ensures equitable opportunities, fosters diversity, and promotes effective conflict resolution.
* Leading the Organization: Understands technology trends, champions alliances, provides support for strategic direction, and fosters a culture of continuous transformation.
* Strategic Technology Planning: Develop plans aligning with organizational needs, incorporating emerging technologies and economic viability.

#### Supervision:

##### Direct Responsibility for the Work of Others:

* Information Security Analyst

**Job Evaluation Factors:**

##### Analytical Reasoning

*Description:*

The role of Director of Information Security in a university environment demands a high level of analytical reasoning. This involves the ability to critically analyze complex information, identify patterns and trends, and make data-driven decisions to enhance the security posture of the university's information systems and assets. The Director must possess strong problem-solving skills and be adept at synthesizing vast amounts of data to assess risks, devise strategies, and respond effectively to security threats and incidents.

*Degree of Complexity or Difficulty of Thinking and Reasoning:* High

*Work Example:*

An example illustrating the requirement for analytical reasoning in the role of Director of Information Security involves conducting a comprehensive security risk assessment for the university's network infrastructure. This assessment involves analyzing various factors such as network architecture, data flow, access controls, threat landscape, and regulatory compliance requirements. The Director must employ analytical reasoning to identify potential vulnerabilities, assess their likelihood and potential impact, prioritize remediation efforts, and allocate resources effectively. This process requires synthesizing information from diverse sources, applying cybersecurity frameworks and best practices, and making informed decisions to mitigate risks and enhance the overall security posture of the university. Additionally, the Director utilizes analytical reasoning when investigating security incidents, analyzing forensic data, and identifying root causes to prevent future occurrences. This ongoing analytical approach is crucial for maintaining a proactive and effective security strategy within the dynamic and evolving landscape of information security threats.

##### Decision Making

*Description:*

The Director of Information Security within a university environment is responsible for overseeing all aspects of information security, including the development, implementation, and maintenance of policies, procedures, and technologies to ensure the confidentiality, integrity, and availability of university data and systems. They collaborate with various departments and stakeholders to assess risks, implement security measures, and respond to security incidents. Additionally, they stay abreast of emerging threats and technologies to continuously enhance the university's security posture.

*Degree of Freedom to Exercise Initiative:* High

*Work Example:*

In the context of a university environment, the Director of Information Security exercises a high degree of freedom to initiate and act independently in making day-to-day decisions. For instance, when a security breach occurs, the Director must quickly assess the situation, determine the appropriate response measures, and coordinate with relevant departments, such as IT, legal, and administration, to mitigate the impact and prevent further damage. In such scenarios, they may need to make critical decisions on the fly, such as whether to isolate affected systems, escalate the incident, or engage external security experts for assistance. Additionally, the Director proactively identifies potential security vulnerabilities and devises strategies to address them, such as implementing multi-factor authentication for sensitive systems or conducting regular security awareness training for university staff and students. This autonomy allows the Director to effectively safeguard the university's information assets while adapting to evolving threats and challenges.

##### Impact

*Description:*

As the Director of Information Security in a university environment, the decisions and actions taken by the incumbent have significant repercussions on the overall security posture and reputation of the department and the university as a whole. The role entails overseeing the protection of sensitive data, intellectual property, and critical infrastructure from cyber threats and attacks. Therefore, the impact of the Director's decisions extends beyond the confines of the department, affecting the entire university community, including students, faculty, staff, and stakeholders.

*Impact or Consequence:* High

*Work Example:*

A typical example demonstrating the impact of the Director's actions involves responding to a large-scale cyberattack targeting the university's network infrastructure. Upon detecting the breach, the Director must swiftly coordinate a response effort involving IT personnel, law enforcement agencies, and external cybersecurity experts. The consequences of their decisions during this crisis can profoundly impact the university in several ways:

*Data Breach Mitigation:* The Director's prompt response and effective containment measures can mitigate the extent of data exposure, minimizing the risk of sensitive information leakage, such as student records, research data, and financial records. Failure to contain the breach adequately could result in severe reputational damage and legal liabilities for the university.

*Operational Continuity:* By making informed decisions to prioritize critical systems and services, the Director ensures minimal disruption to academic and administrative operations. Timely restoration of essential services such as online learning platforms, email systems, and research databases is crucial to maintaining the university's functionality and reputation as an educational institution.

*Reputation Management:* The Director's handling of the cyberattack directly impacts the university's reputation among students, parents, alumni, donors, and the broader academic community. Transparent communication, effective crisis management, and proactive measures to prevent future incidents are essential for safeguarding the university's credibility and trustworthiness.

*Financial Implications:* The financial repercussions of a cyberattack can be substantial, including remediation costs, legal expenses, regulatory fines, and potential loss of revenue due to diminished enrollment or research opportunities. The Director's decisions regarding resource allocation and risk mitigation strategies directly influence the financial resilience of the university in the aftermath of a security breach.

##### Responsibility for the Work of Others

The Director of Information Security plays a crucial role in supervising and leading a diverse team of professionals, ensuring that the hiring, performance evaluations, coaching, and disciplinary actions are aligned with the department's objectives and the university's overall mission. This factor underscores the director's responsibility for fostering a collaborative and high-performing team that contributes to the success of the IT team.

* Information Security Analyst

##### Communication

*Description:*

Effective communication is essential for the Director of Information Security in a university environment to ensure alignment with organizational goals, facilitate collaboration, and disseminate critical information related to cybersecurity. The role involves regular interaction with various internal stakeholders within the university, as well as external partners and entities involved in cybersecurity initiatives and compliance.

Key Internal Communication Partners:

1. University Administration: The Director communicates with university administrators, including the President, Provost, Vice Presidents, and Deans, to provide updates on the university's security posture, discuss strategic initiatives, and seek support for cybersecurity projects and resource allocation.
2. Information Technology (IT) Department: Collaboration with the IT department is essential for implementing security measures, addressing vulnerabilities, and responding to security incidents. The Director liaises with IT staff, including network administrators, system engineers, and helpdesk personnel, to ensure alignment between security policies and technical implementations.
3. Academic Departments and Research Centers: Engaging with academic departments and research centers enables the Director to understand unique security requirements, provide guidance on securing research data, and foster a culture of security awareness among faculty, researchers, and students.
4. Human Resources (HR) Department: Communication with the HR department involves coordinating security awareness training programs, disseminating security policies and procedures, and collaborating on employee onboarding and offboarding processes to ensure compliance with security protocols.

Key External Communication Partners:

1. Government Agencies and Regulatory Bodies: External communication with government agencies, such as the Department of Education and regulatory bodies like the Higher Education Information Security Council, involves reporting security incidents, seeking guidance on compliance requirements, and participating in collaborative efforts to enhance cybersecurity in higher education.
2. Industry Partners and Vendors: Collaboration with industry partners and cybersecurity vendors involves sharing best practices, evaluating new security technologies, and negotiating contracts for security products and services that meet the university's needs.
3. Peer Institutions and Professional Organizations: Engaging with peer institutions and professional organizations, such as the CANSOC, ONCHEH,

facilitates knowledge sharing, benchmarking, and collaboration on cybersecurity initiatives and research.

##### Effective communication with these internal and external partners is crucial for the Director of Information Security to promote a culture of cybersecurity awareness, address emerging threats, and safeguard the university's digital assets and reputation.

##### Motor/ Sensory Skills

Description: While the role of the Director of Information Security involves cognitive and managerial tasks, there are certain motor and sensory skills required to perform specific duties effectively. Proficiency in these skills ensures the smooth execution of tasks related to the oversight and management of information security operations within the university.

Level of Proficiency or Precision Required: Low to Moderate

Tasks Requiring Motor/Sensory Skills:

1. Keyboard and Mouse Operation: The Director may need to use a computer extensively for tasks such as reviewing security reports, analyzing data, and communicating with stakeholders via email or other digital platforms. Proficient use of a keyboard and mouse is necessary for navigating through various software applications and inputting information accurately.
2. Presentation Delivery: Delivering presentations to university stakeholders, including administrators, faculty, and staff, requires effective verbal communication skills and the ability to use presentation software (e.g., PowerPoint). The Director must be capable of operating presentation equipment, such as projectors or screens, to convey information clearly and engagingly.
3. Collaborative Meetings: Participating in collaborative meetings with internal and external partners involves active listening, note-taking, and effective verbal communication. The Director must be attentive during discussions, take accurate notes, and contribute meaningfully to the conversation while maintaining professionalism and diplomacy.
4. Visual Inspection: While not as prominent as in some other roles, the Director may need to visually inspect physical security measures, such as surveillance cameras, access control systems, or security hardware installations, to ensure compliance with security standards and protocols.
5. Reviewing Documentation: Reviewing security policies, procedures, and documentation requires visual acuity and the ability to comprehend complex technical information presented in written form. The Director must be able to read and interpret documents accurately to assess their effectiveness and relevance to the university's security objectives.
6. Coordinating Security Drills: Organizing and participating in security drills or exercises, such as tabletop simulations or incident response scenarios, may involve physical movement and coordination to ensure participants understand their roles and responsibilities during simulated security incidents.

##### Effort

*Description:*

The role of Director of Information Security in a university environment demands both physical and mental exertion in the ordinary course of performing duties. While the position primarily involves mental tasks related to strategic planning, risk assessment, and policy development, there are instances where physical effort and sustained mental focus are required to effectively manage information security operations.

Physical and/or Mental Demands:

1. Sustained Concentration and Focus: The Director must maintain a high level of concentration and focus when analyzing security data, assessing risks, and making critical decisions regarding the protection of university assets. Sustained mental effort is required to identify emerging threats, evaluate security controls, and develop mitigation strategies to safeguard against potential cyberattacks.
2. Problem-Solving and Decision-Making: Addressing complex security challenges and responding to security incidents necessitates strong problem-solving skills and the ability to make timely and effective decisions under pressure. The Director must analyze situations quickly, evaluate available options, and implement appropriate courses of action to mitigate risks and minimize impact on university operations.
3. Communication and Collaboration: Interacting with various internal and external stakeholders involves effective verbal and written communication skills, as well as the ability to collaborate with multidisciplinary teams. The Director must convey technical information clearly and concisely, engage in diplomatic negotiations, and build consensus among diverse stakeholders to achieve security objectives.
4. Managing Workload and Priorities: Balancing competing priorities, deadlines, and resource constraints requires effective time management and organizational skills. The Director must allocate resources efficiently, delegate tasks appropriately, and adapt to changing circumstances to ensure the timely completion of security initiatives and projects.
5. Remain Current with Technology and Trends: Staying abreast of emerging technologies, threat actors, and cybersecurity trends requires continuous learning and professional development. The Director must dedicate time and effort to research, training, and networking within the cybersecurity community to enhance knowledge and skills and apply best practices effectively within the university environment.
6. Leading and Motivating Teams: Inspiring and motivating security teams to achieve departmental goals and objectives requires strong leadership skills and emotional intelligence. The Director must foster a collaborative and inclusive work environment, provide guidance and mentorship to team members, and resolve conflicts or challenges that may arise during the course of operations.

While the role of Director of Information Security primarily involves mental tasks such as analysis, planning, and decision-making, it also requires physical effort in terms of effective communication, collaboration, and leadership, as well as sustained mental focus to manage the complexities of information security within a university environment.

##### Working Conditions

The working conditions factor for the Director of Information Security role considers a combination of sedentary work, high cognitive demands, ambiguity, collaboration pressures, technology implementation challenges, institutional responsibilities, work-life balance considerations, and data security stressors.

*Working Conditions:*

1. Sedentary Work Environment:
   * Nature: A predominantly sedentary role requiring prolonged periods of deskwork and computer usage.
   * Frequency and Duration: Daily exposure to desk-based tasks, with occasional breaks.
2. High Cognitive Load:
   * Nature: The need for sustained mental concentration and focus on complex technical and strategic matters.
   * Frequency and Duration: Daily exposure to intricate problem-solving, decision-making, and strategic planning.
3. Ambiguity and Uncertainty:
   * Nature: Inherent uncertainty in technology projects, with unforeseen challenges and evolving academic needs.
   * Frequency and Duration: Regular exposure to ambiguity, necessitating adaptability and flexibility.
4. Meeting and Collaboration Demands:
   * Nature: Engaging in frequent meetings, discussions, and collaborations with various stakeholders.
   * Frequency and Duration: Regular exposure to team interactions, requiring effective communication and collaboration skills.
5. Technology Implementation Pressures:
   * Nature: Pressure associated with the successful implementation of enterprise applications within specified timelines.
   * Frequency and Duration: Occasional exposure to critical project phases, demanding focused efforts.
6. Responsibility for Institutional Impact:
   * Nature: Decision-making with broad institutional implications, adding a high level of responsibility.
   * Frequency and Duration: Ongoing exposure to decisions that directly impact the university's operations and academic functions.
7. Work-Life Balance Challenges:
   * Nature: The potential for extended working hours and occasional challenges in maintaining work-life balance.
   * Frequency and Duration: Occasional exposure during critical project phases or issue resolution.
8. Data Security and Compliance Stressors:
   * Nature: The responsibility for data security and compliance introduces stressors related to safeguarding sensitive information.
   * Frequency and Duration: Regular exposure to addressing and mitigating potential security risks to protect the university's data.