Professional Position Description

Section I Position Information	Update Only ☐ Classification Review ☒
Position Title	Digital Security Office Management Officer
Position #	
Department	Digital Security Office
Classification Level	Excluded B
Reports to	Chief Information Security Officer and Digital Security Office
Effective Date	
Position Summary Briefly describe the main purpose(s) of the position	Reporting to the CISO/Digital Security Office, the Digital Security Office Management Officer (DSOMO) will coordinate all CISO/DSECO activities in support of functional priorities such as strategic plans, initiatives, and organizational development processes. The DSOMO will assist in maximizing the effective operation of the Digital Security Program (DSP) with respect to workflow, scheduling, teaming, budget, communications, and events. The DSOMO creates necessary ad hoc reports, leads briefings, creates presentations, and responds to DSecO strategic issues. The incumbent provides operational guidance to the CISO/DSECO and develops detailed work plans for the completion of tasks while acting as project lead for DSecO projects that are key to functional and strategic success. Conducts program status with Deputy Digital Strategy Office/CISO and DSP program sponsor in support of AU goal; and shall organize training and development initiatives for the DSecO team. The DSOMO shall provide feedback on the, coaching, and development of the DSecO team to the Director, Digital Security Office (DDSO). The DSOMO will be the primary liaison with AU's audit, compliance, privacy, and regulatory functions and will manage operational deliverables required to fulfill the DSP's audit reporting accountabilities including preparation of quarterly implementation status updates on Office of the Auditor General Observations and Internal Audit recommendations owned by DSecO reviewed by CISO/DSECO and submitted to VPITCIO for Board of Governors reporting.
Duties and Responsibilities Organize by key responsibility area and include % of time spent where possible	• Collaborates with internal and external auditors to conduct compliance audits of security practices, policies, procedures, and standards • Works with CISO/DSECO to facilitate Digital Security Program (DSP) governance through the implementation of an AU security governance program that not only matches the digital business objectives of AU, but also responds to external extenuating factors and rapidly adapts to ensure risks to AU do not exceed tolerance levels • In collaboration with CISO/DSECO and Senior Technical Project Managers: Security, prepares detailed operating and financial

	reports in support of strategic, operational, and functional deliverables • In collaboration with Senior Technical Project Managers: Security, receives and reports on monthly project financials as created by Cloud Business Office Project Budgets Analyst.Participates in program status reviews with Deputy, Digital Strategy Office/CISO and DSP program sponsor in support of AU goals. • Supports the implementation and maintenance of AU IT policies • Participates in risk review monitoring and reporting • Works with CISO/DSECO and DSP team to develop and report on management and executive level cybersecurity risks • Monitors progress towards achieving improvement plans for the overall functioning of the Digital Security Office and its communications with other area of the IT division and key non-technical stakeholders and program owners across the university. • Interacts with Directors and Executive to build an understanding of, and support for, IT security measures • Works with CISO/DSECO and Security Awareness Analyst to provide guidance and advice related to digital security to all faculties and administrative units of the university • Works with CISO/DSECO, Director, Digital Security Office and Security Awareness Analyst in collaboration with the Cloud Business Office Manager, Technical Service Training to curate and develop online and virtual digital literacy curriculum related to cybersecurity awareness for AU staff and students to be provided by Technical Service Trainers and Security Awareness Analyst • In coordination with the Director, Digital Security Office and the Manager, Digital Strategy Architecture and Governance, develop, implement, and monitor a strategic, comprehensive enterprise information security and IT risk management program to ensure that the integrity, confidentiality, and availability of information is owned, controlled, or processed by the organization • Participates in the development, maintenance, and publishing of up-to-date AU standard operating procedures • Supports the Security Awareness Analyst in the curation/development of security awareness and training content • Works with AU security vendors to create, communicate, and implement a risk-based process for vendor risk management, including the assessment and treatment for risks that may result from partners, consultants, and other service providers • Supports the CISO/DSECO, Director, Digital Security Office and Senior Technical Project Managers: Security in reviewing and managing DSecO budgets and monitoring for variances • Creates and manages a unified and flexible control framework to integrate and normalize the wide variety and ever-changing requirements resulting from laws, standards, and regulations

	• Ensures that security programs are in compliance with relevant laws, regulations, and policies to minimize or eliminate risk, audit, and compliance findings • Monitors the external threat environment and externally-supplied threat intelligence briefings for emerging threats, and advises DSecO team on the appropriate courses of action • Facilitates a metrics and reporting framework to measure the efficiency and effectiveness of the DSecO's Digital Security Program and other cybersecurity –related projects and initiatives towards increasing the maturity of AU's cybersecurity • Understands and interacts with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems, and services, including, but not limited to privacy, risk management, compliance, and business continuity management • Provides weekly status updates to the CISO/DSECO and Director, Digital Security Office • Tracks and reports on DSecO operational project controls implementation drift, and improvement opportunities • Accountable for ensuring own and all DSecO staff enter their internal labour on operating and capital initiatives via use of ServiceNow time reporting. • Closely collaborates with the Cloud Business Office Management Officer and the Cloud Business Office Licensing Specialist regarding requisition, purchase order and invoicing processes for all DSecO external contracts. • Supports the CISO/DSECO and Director, Digital Security Office in the Request for Proposal (RFP) processes related to creating, issuing, reviewing, and rewarding RFPs for external services in coordination with the Cloud Business Office Licensing Specialist and the AU Office of Procurement. • Closely collaborates with the Cloud Business Office Management Officer on administrative activities related to all financial and HR processing for the DSecO of the IT division
Occupational Health and Safety	Employees: Responsible to participate in the AU OHS Program as required. Supervisors: Responsible for awareness of one's OHS Responsibilities as an AU employee and supervisor, for participating in the AU OHS Program as required, and for ensuring the participation of employees in the AU OHS Program as required. See: https://ohs-pubstore.labour.alberta.ca/li008
Classification Factors	
Communication	Excellent communication and organizational skills, as the DSOMO is responsible for developing and maintaining effective working relationships with a variety of internal and external individuals and groups including but not limited to: the OVPIT&CIO division, vendors, the

	AU Privacy Officer, the AU Internal Auditor, the AU Director of Strategic Initiatives who is accountable for the AU Enterprise Risk Framework and AU staff. Must be able to gather, interpret and act upon information from various sources. Able to demonstrate maturity of judgment of prioritizing problems that may arise and convey these to the DDSO/CISO and Director, Digital Security Office where necessary. Knowledge and implementation of Digital Governance Control Framework for IT Policy and Procedures, other department policies and procedures, and an understanding of FOIP policy.
Supervision	May supervise cybersecurity vendors and interns and summer students
Impact of Service or Product	High level of personal integrity, with the ability to handle confidential and otherwise sensitive matters professionally and with the appropriate level of judgement and maturity.
Independence of Action	As the DSOMO deals with all divisions of the University, s/he must maintain a high degree of confidentiality regarding matters that may impact risk to the University IT division. Adherence to deadlines and schedules supports the effective operation of the Digital Governance Committee and subcommittees, Project Steering Committees, Executive Group and other Committees, Incorrect advice or information could have a substantial negative impact. Priorities assigned to DSecO activities across the division impact the timely and efficient delivery of projects and operational services to the university community. Accuracy of information related to cybersecurity risk and DSecO matters could impact the reputation and standing of the university.
Complexity	Complexity derives from the multiple stakeholders involved in typical security governance and operations. The DSOMO must consider stakeholder concerns, and work with the CISO/DSECO and Director, Digital Security at all times to manage expectations. Must be able to effectively prioritize and execute tasks in a high-pressure environment.
Planning	Working from a list of priorities as defined in the Integrated Resource Planning (IRP) process of AU and under the guidance of the CISO/DSECO and Director, Digital Security Office, the DSOMO develops DSecO plans that include a wide variety of input variables and processes. The plans must be sufficiently detailed to allow accurate budgets and schedules to be drawn up.

Signatures for Section I

Incumbent's Signature _____ Date _____

Supervisor's Signature _____ Date _____

Section II
Qualifications

Includes education, experience, skills, abilities and any other special qualifications required. The qualifications relate to the position not the incumbent

- Minimum of five years' experience in a Security or Compliance administrative role in IT, Compliance or Legal division of corporate or public sector organizations required
- AWS Cloud Practitioner Certification required
- AWS Certified Security Specialty certification preferred
- Minimum of five years' experience in another IT function preferred
- Minimum of five years' experience with regulatory compliance, cybersecurity frameworks and standards (ISO27000, COBIT, NIST 800, etc.) preferred
- Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM) preferred
- Diploma or degree in computer science, management, or engineering, recognized in Canada. In lieu of a degree or diploma, additional experience over and above the minimum requirement may be considered.
- Understanding of cybersecurity risk management and risk mitigation strategies
- Ability to communicate project and technology risks effectively
- Strong negotiation skills to negotiate resources, changes, issues, budgets, and timelines
- Passionate about customer service excellence
- Multi-tasking ability, must be comfortable with simultaneously managing multiple initiatives
- Excellent interpersonal, communication, leadership, motivational, organizational, and planning skills
- Resourceful, creative, attentive to detail, self-directed and self-motivated
- Strong problem-solving skills, including the ability to take a practical approach to dealing with shifting priorities, demands, and timelines
- Extensive experience working in a team-oriented, collaborative environment

Signatures for Sections I and II

Department Head Signature _____ Date _____

Executive Officer Signature _____ Date _____

Human Resources Review _____ Date _____