Information Security Risk and Compliance Lead

REPOST
Forbes includes U of G Among Canada's Best Employers
Professional and Managerial Group

Information Security Risk and Compliance Lead

Computing and Communications Services

Hiring #: 2021-0043

Please read the Application Instructions [1] before applying

Computing and Communications Services (CCS) is the central IT department at the University of Guelph, providing core IT services and technology solutions to the University community. CCS has a progressive organizational culture, including a strong learning and development focus, and is committed to its Core Values of Service Culture, Integrity, Individual Leadership, Teamwork, Agility, and Communication.

Reporting to the Chief Information Security Officer (CISO) within the Computing and Communications Services (CCS) department, the Information Security Risk and Compliance Lead is a senior position primarily responsible for providing subject-matter expertise and leadership of the information security policy, risk, compliance, and security awareness portfolios. The successful candidate will be responsible for influencing direction, developing consensus, and the planning and execution of initiatives in these areas to support the overall cyber security roadmap of the University.

Working in conjunction with other members of the Information Security team, campus IT groups, management, faculty, and staff, this position has responsibility for:

- Providing subject-matter expertise and consultation services to University departments regarding data and systems security, risk management, and standards compliance. This includes representing Information Security on projects and working groups, such as the Research Ethics Board (REB), where they will provide consulting services and thorough review of information and data security concerns.
- Assessing the security and risk associated with proposed new platforms and applications, including cloud-based services, as requested by campus units or individual members of the campus community. The review process will include analyzing technical documentation, request for proposal (RFP) responses, technical architecture, third party security reports, and vendor responses to security assessment questions.
- Leading CCS efforts on our governance, risk, and compliance activities including ongoing support for the associated processes and tools. This includes tracking audit findings with staff and preparing a monthly metrics dashboard for management and internal audit. This also includes working with groups on campus and with auditors to ensure that we adhere to and maintain our certifications, such as our annual PCI compliance certification.
- Managing investigations into information security incidents and violations of University information security policies. This includes documenting and tracking these incidents, along with interfacing with management, Campus Community Police, University committees, and external agencies as necessary.
- Leading cyber security awareness initiatives to educate students, staff, and faculty on secure computing practices. This will include giving presentations to campus groups on relevant topics, including new employee orientation presentations and other security awareness events during the year.
- Overseeing the response and remediation of security vulnerabilities with system owners and campus IT representatives as part of the information security vulnerability management program. Specifically, this position will work with system owners to drive closure of security vulnerabilities to improve the overall security posture of the University.
- Auditing and formulating security standards, policies and procedures related to all aspects of information security.

- As a member of the Security Operations Centre (SOC) team, regularly assessing and proactively monitoring the security and risk posture of University information systems, networks, technical infrastructure, accounts, and data.
- Participating in the evaluation, acquisition and implementation of security related technologies, such as authentication/authorization mechanisms, encryption, certificate services, anti-malware software, email and network filtering, intrusion detection, and security information and event management.
- Collaborating with the CISO to develop security roadmaps, project plans, and risk mitigation strategies.

Requirements of the position include:

-
-

- Bachelor’s degree in Computer Science, Information Technology, Math, Business Administration, or related field, and a minimum of seven (7) years of related work experience
- Extensive prior work experience in cyber security roles
- Expert knowledge and hands-on technical experience in cyber security monitoring, incident handling, response, and investigation
- Demonstrated expert knowledge and understanding of all information security domains:
    - Security and risk management
    - Asset security
    - Security architecture and engineering
    - Communications and network security
    - Identity and access management
    - Security assessment and testing
    - Security operations
    - Software development security
- Previous experience performing security risk assessments and vulnerability management
- Strong ability to analyze and understand technical data, including white papers, proposals, and RFPs
- Experience and familiarity with disaster recovery methodologies, business resumption planning, and application development methodologies
- Familiarity with relevant Canadian and International privacy legislation and standards such as ISO 27001, FIPPA, PHIPA, and PCI-DSS
- Demonstrated ability to exercise sound and ethical judgement when handling matters requiring high level of diplomacy, sensitivity and confidentiality
- Highly developed skills of collaboration, communication (written and oral) and time management, with an ability to explain complex concepts to technical and non-technical members of the University community
- Strong leadership, business analysis, and project management skills
- Strong customer service focus and solution orientation
- Strategic thinking with proven analytical and creative problem solving skills
- Demonstrated ability to establish priorities with a track record of delivering on strategic and tactical objectives
- Ability to work well under pressure, meet established deadlines, and manage conflicting priorities
- Ability to work individually and as an integral member of a high-performance team

The following skills and experiences will set a candidate apart:

- Industry recognized information security certifications, such as CISSP, CISM, GIAC, PCIP, or equivalents
- Previous experience in higher education
- Familiarity with the information technology needs of a University community and an understanding of the work environments, policies, and governance structures of a University
- Prior experience in supporting users in a large, complex, institutional information technology environment, in the area of information security

This appointment is regularly performed on- campus but will be initially fulfilled remotely (off-campus) until the University resumes its regular operations.

Position Number 504-005
Classification P07*
Professional/Managerial Salary Bands [2]

*Tentative evaluation; subject to committee review.

At the University of Guelph, fostering a culture of inclusion** [3] **is an institutional imperative. The University invites and encourages applications from all qualified individuals, including from groups that are traditionally underrepresented in employment, who may contribute to further diversification of our Institution.

Posting Date: 2021 04 26
Closing Date: 2021 05 10

Keywords: current.opportunity [4]

Links
[1] https://www.uoguelph.ca/hr/careers-guelph/how-apply
[2] https://www.uoguelph.ca/hr/system/files/2020-2023%20P%26M%20Salary%20Grid_2.pdf
[3] https://www.uoguelph.ca/diversity-human-rights/sites/uoguelph.ca.dhr/files/public/Inclusion%20Framework%20Endorsed%20April%202017.pdf
[4] https://www.uoguelph.ca/hr/tags/currentopportunity