Manager, Cybersecurity and Policy Advisor

Capilano University is named after Chief Joe Capilano (1854–1910), an important leader of the Skwxwú7mesh (Squamish) Nation of the Coast Salish Peoples. We respectfully acknowledge that our campuses are located on the unceded territories of the səlilwətaɬ (Tsleil-Waututh), shíshálh (Sechelt), Skwxwú7mesh (Squamish), and xʷməθkʷəy̓əm (Musqueam) Nations.

At Capilano University we are committed to supporting a campus community that is both diverse and inclusive. We believe that diversity within our workforce is essential in creating both an exceptional student and employee experience. As part of our ongoing commitment to Diversity, Equity and Inclusion (DEI), we strive to ensure that our recruitment campaigns authentically reflect the diverse community we serve. We actively encourage applications from Indigenous Peoples, Black and racialized persons, persons with disabilities, women, and members of the 2SLGBTQIA+ community, as we value the unique perspectives, lived experiences, and skillsets each individual brings to CapU.

To help us focus our efforts, we encourage all applicants to complete a short anonymous questionnaire, if they wish. The results of the questionnaire are not linked to you or your application and do not form part of the selection process. The goal of collecting this anonymous data is to gain a better understanding our organizational reach, while continuously working to improve the diversity of our applicant pool.

All qualified candidates are encouraged to apply; however, Canadians and permanent residents will be given priority. Should you require accommodations during the hiring process please reach out to mimibuan@capilanou.ca (Ad/Ex and Staff).

Position Title: Manager, Cybersecurity and Policy Advisor

Employee Group: Administrator

Department: Digital Technology Services

Position Status: Regular Full-Time

Position Number: A99990

Position Start Date: ASAP

Job Posting Open Date: January 7th, 2026

Job Posting Close Date: Open until filled

Pay Group: 11

Location: North Vancouver

Working with us

As a member of the Digital Technology Services (DTS) team here within Capilano University, you will be a vital asset in providing an exceptional experience to both our employee and student communities through invention, collaboration, and technical talent.

As we embark on our university wide digital transformation, we'll be seeking fellow trailblazers to join our teams as we integrate state of the art technologies. With a variety of projects and initiatives in the pipeline, there is no shortage of opportunity to innovate.

Within our teams, you'll be working alongside a variety of talented individuals involved in initiatives focused on cyber security, data analysis, operational analytics, quality assurance, integration, customization, and implementation.

Do you have a passion for optimization? Join us in creating a lasting impact that goes beyond routine tasks, contributing to the long-term success of our technological landscape and the university community.

About the role

Reporting to the Director of DTO and Cybersecurity, Digital Technology Services, (DTS) and a part of the Associate Vice President (AVP) DTS leadership team, the Manager, Cybersecurity and Policy Advisor leads the cybersecurity team that provides cybersecurity governance and policies to digital solutions across the university.

This role will have the opportunity to influence and drive lasting efforts in the University's digital transformation, with significant student and employee impact through the management and monitoring of a robust cybersecurity program and development of policies relating to digital solutions. In close alignment with university-wide strategy, critical components of this position include updates to the cybersecurity strategy, risk management framework, vulnerability management program, cybersecurity protection, cybersecurity access controls, cybersecurity detection and incident response plan. The role requires a strong focus on building and maintaining relationships both across the CapU community and externally with sector colleagues and vendors.

KEY RESPONSIBILITIES

- In consultation with the Director, DTO and Cybersecurity, plans implements, and manages cybersecurity governance that is guided by cybersecurity frameworks, critical security controls and the National Cybersecurity Assessment (NCA) framework.
- Develops and manages policies and guidelines relating to cybersecurity which all digital solutions must adhere to.

▪ Proactively contributes to technical assessments from a cybersecurity perspective of all digital solutions that are being selected for the digital ecosystem. This includes providing security requirements and performing evaluations from a cybersecurity perspective for RFPs.
▪ Develops DTS policies and manages these in a central repository. Conducts annual reviews of all DTS policies to ensure relevance.
▪ Develops and manages the cybersecurity sections of technical assessments.
▪ Leads and coordinates an appropriate level of response to cybersecurity alerts and incidents, including the implementation and review of a cybersecurity incident response plan. ▪ Identifies and selects appropriate cybersecurity monitoring tools to ensure no gaps exist in security management across the digital ecosystem. ▪ Proactively monitors the digital ecosystem using industry standard tools to detect malware, suspicious activity, and breaches across all levels of the digital ecosystem, including network, services and applications

Experience, competencies & qualifications

KEY COMPETENCIES
▪ Job knowledge: knowledge and experience with cybersecurity best practices; demonstrates proven leadership experience in developing strategies, plans, programs and policies related to the delivery of cybersecurity strategy and operations.
▪ Service focus: understands the role of cybersecurity and digital solutions, and how change affects teams and processes; delivers services that align with the DTS roadmap that support the university's key priorities of exceptional student and employee experience.
▪ Result oriented: feels personally committed and accountable to deliver results quickly, accurately, and effectively; uses thoughtful judgement when responding to situations that are not going well and uses foresight to overcome obstacles.
▪ Initiating action / taking initiative: embraces a continuous improvement mindset in an ongoing effort to improve services and processes; readily acts consistent within departmental or university objectives; volunteers readily and takes independent actions when appropriate.
▪ Leadership and supervisory abilities: encourage and supports cross-functional, high-performing teams; attracts and selects the best talent; coaches and inspires people; sets expectations, recognizes achievement, and proactively manages conflict

EDUCATION / TRAINING AND EXPERIENCE
▪ 5+ years of relevant professional experience, with 1 years in a recent leadership role with direct responsibility for a cybersecurity program, preferably in a public sector environment.
▪ Demonstrated experience in leading a cybersecurity program.
▪ Demonstrated experience and knowledge of cybersecurity processes, tools, and procedures, including policies and establishing governance structures.
▪ A bachelor's degree
▪ Industry relevant designations such as CISSP, CISA, CRISC, ITIL, TOGAF.
▪ Experience with the ITIL framework an

For more information, please see the complete job description (*Include hyperlink to job description****.***

Benefits

At Capilano University, we understand that there is more to life than work. That is why we offer comprehensive benefits and support to help you and your family live a balanced life. Take a sneak peak to see what it is like to work at Capilano University.

Days and Hours of Work:

Will depend on the position status, but typically will include the following:

Our standard work week is Monday to Friday, 8:30am – 4:00pm, or dependent on the needs of the department.

Salary: The typical salary range for this role falls between **$92,139 – $122,852** per annum, commensurate with experience, education, and internal equity, with future opportunities for performance-based pay and career progression.

Capilano University also offers a competitive total rewards package (college pension plan, employer paid benefit premiums, health spending account, modified work week, remote working options etc).

How to apply

Please submit your application package to talentacquisition@capilanou.ca and be sure to included the following:

1) The position tile and position number in the subject line of your email. Ex: *HR Advisory – Talent Acquisition – A00000*
2) Your resume and cover letter. We will let you know if we require any further documents for your application, such as proof of education, for example.
3) Your responses to the supplemental questions shared below. Please include both the question and your response in the body of the email:
    a. Are you legally entitled to work in Canada? (i.e. valid work permit, permanent resident, Canadian citizen) (required)
    b. Do you have a bachelor's degree? (Yes or No)
    c. Do you have 5+ years of relevant professional experience, with 1 years in a recent leadership role with direct responsibility for a cybersecurity program

Thank you for your interest in this opportunity with us at Capilano University!