Employment opportunity: Information Technology Security and Compliance Specialist

Are you an Information Technology (IT) Security and Compliance professional interested in working for a progressive health care union with a large and diverse membership, and a broad social justice mandate?

The Hospital Employees' Union is looking for an experienced **IT Security and Compliance Specialist** to work at its provincial office in Burnaby, British Columbia.

Reporting to the Director of Information Technology, the IT Security and Compliance Specialist will be responsible for the developing, implementing, and maintaining the organization's information technology security policies, procedures, and compliance programs.

This role involves safeguarding the company's digital assets, ensuring compliance with industry regulations, and mitigating risks associated with information security.

Duties and Responsibilities

1. Policy Development and Implementation:
    - Develop, review, and implement IT security policies, standards, and guidelines to ensure the organization's information systems are secure and compliant with relevant laws and regulations.

2. Compliance Management:
    - Monitor and enforce compliance with industry regulations, standards, and legal requirements related to information security and data privacy.
    - Stay updated on changes in regulations and adjust organizational policies and practices accordingly.

3. Risk Assessment and Mitigation:
    - Conduct regular risk assessments and vulnerability analyses to identify potential risks to the organization's information assets.
    - Develop strategies and implement measures to mitigate identified risks effectively.
    - Coordinate and conduct regular security audits, vulnerability assessments, and penetration testing to identify vulnerabilities and weaknesses in the organization's IT systems.

- Collaborate with internal and external stakeholders to remediate identified security gaps.

4. Security Incident Response:
    - Develop and maintain an incident response plan to promptly address and manage security incidents, breaches, and other emergencies.
    - Investigate security incidents and breaches, assess the impact, and implement necessary actions for resolution and prevention of future occurrences. Maintain thorough documentation of security incidents, investigations, and remediation efforts.
    - Prepare and present comprehensive reports on security status, incidents, and compliance to senior management and relevant stakeholders.

5. Security Awareness and Training:
    - Develop and deliver training programs and awareness campaigns to educate employees about security policies, best practices, and potential threats.
    - Foster a security-conscious culture within the organization.

6. Access Control and Monitoring:
    - Establish and manage access control mechanisms, ensuring that only authorized personnel have access to sensitive systems and data.
    - Monitor and analyze access logs to detect suspicious activities and potential security breaches.

7. Security Technology Evaluation:
    - Evaluate and recommend security technologies and tools to enhance the organization's security posture.
    - Work closely with IT team to implement and manage security solutions effectively.

Qualifications and Experience

Bachelor's degree in Information Technology, Computer Science, or a related field. Advanced degrees or certifications in security (e.g., CISSP, CISM, CISA) are highly desirable.

Proven experience (7+ years) in information security, compliance management, and risk assessment within an organizational setting.

In-depth knowledge of relevant laws, regulations, and industry standards related to IT security and compliance (e.g., PIPEDA, HIPAA, ISO 27001).

Strong analytical and problem-solving skills, as well as excellent communication and interpersonal abilities.

Ability to work effectively in a team, manage multiple projects simultaneously, and adapt to a dynamic and fast-paced environment.

May be required to work some evenings and weekends and may be required to travel.

Must be legally able to work in Canada (i.e. Canadian citizenship, permanent residency, or valid work permit)

This is a unionized position. Compensation is based on a collective agreement and includes a 72-hour fortnight and generous vacation time and benefits, including a defined benefit pension plan. The current annual salary for this position is $107,677.44.

About HEU

Since 1944, the Hospital Employees' Union has advocated for better working and caring conditions, defended public health care, and stood against privatization.

We have a long history as a strong, democratic, progressive, socially conscious union committed to social justice and advancing labour and human rights on a local and global level. We identify and challenge historical and systemic inequities and hear, respect, serve, empower, and advocate for each and every member. Together we fight for fairness, solidarity, equity, inclusion, and understanding, knowing that our members' economic security depends on our success.

HEU is an equal-opportunity employer. We are committed to being a workplace that is free of discrimination, values diversity, and is representative of the communities we serve. HEU encourages applications from members of historically marginalized groups: 2SLGBTQ+, Indigenous, Black, and people of colour, persons with disabilities, young workers, and those who identify as women.

Interested in working with us? Here is how to apply.

Please send your resume and cover letter **by 4 PM on Thursday, June 6, 2024,** to: **Jobapplication@heu.org (subject line: IT Security and Compliance Specialist – Your Name).**

Please note that due to the anticipated volume of applications, we will only be responding to applicants selected for an interview.