Cyber Security Officer

Department:	IT Services	**Competition #:**	23-SS-02
Campus:	South - Windsor	**Classification:**	Support Staff
Posting Type:	Internal/External	**Payband:**	K
Status:	Full Time	**Hourly Rate:**	$42.38 – $49.15
Position Testing:	Yes	**Hours Per Week:**	37.5 hours Monday to Friday, 8:00am – 4:00pm
Clerical Testing:	No		
Start Date:	As soon as possible	**Closing Date:**	Friday, January 13, 2023 by 4:30pm

St. Clair College is seeking an experienced and motivated professional who shares our commitment to quality and student success.

POSITION SUMMARY

Under the supervision of the Manager Network & Security, the incumbent is responsible for ensuring that electronic information is secure and appropriately protected, and the methods and devices that provide technology services meet the College's security standards. The incumbent provides IT security consulting, leadership and coordination related to the securing and risk mitigation of IT technologies used by employees and students throughout the college. He/she is responsible for analyzing and resolving security breaches and vulnerability issues in a timely and accurate fashion, leading ad hoc Security Incident Response Teams and conducting user activity audits.

The incumbent will deal with information of a highly sensitive and confidential nature on an ongoing basis, including when investigating incidents and security breaches. The incumbent will deal with highly complex situations.

CORE DUTIES & RESPONSIBILITIES

Monitoring, Testing, and Reports **40%**

- Conducts IT security monitoring and administrative activities for IT infrastructure, servers, systems and applications, data integrity and compliance with defined security parameters for systems. The incumbent will identify systems behavioural trends which may suggest a breach of IT security, often heuristically.
- Conducts vulnerability and penetration testing to determine the organization's security posture, initiating appropriate follow-up action.
- Conduct and draft post-mortem analysis reports, subsequent to major events, outlining root cause, lessons learned, and mitigation action. Drafts policies, operative norms and guidelines for senior management approval. Compliance to IT security-related policies and procedures may be audited by the incumbent on an occasional or as-required basis.

Systems and Applications **30%**

- Works with ITS systems administrators responsible for College computer systems, taking leadership to ensure that systems and applications are appropriately secure and protected. Incumbent will define parameters and/or operative norms for the setup and support of these systems.

Customer Support **20%**

- Assesses customer needs in accordance with industry IT security best practices and establishes guidelines for appropriate solutions. Ensures that IT solutions meet College objectives while remaining compliant with IT security standards.

Other duties as assigned **10%**

MINIMUM QUALIFICATIONS

EDUCATION

The ideal candidate must possess a minimum of a four (4) year degree in Information Technology, Networking, Cyber Security, or equivalent.

EXPERIENCE

The ideal candidate must possess a minimum of five (5) years' in-depth work experience in an enterprise or campus environment with computer workstations, servers, networks, and operating systems. Experience in the implementation and enforcement of IT security practices in an enterprise environment. Experience working with external auditors and IT security consultants. This must include a minimum of three (3) years' training in Windows Server security, network security, and IT security practices in an industry-recognized curriculum (CISSP, CEH).

In order to be considered, internal applicants must be in good standing as defined in the College's Recruitment & Selection Policy.

ANALYSIS & PROBLEM SOLVING

- A system or service is exhibiting unpredictable behaviour.
- "Phishing" attempts (fraudulent emails that appear to be sent from legitimate organizations.
- IT Security risk reduction. Signal need to perform vulnerability patching on core servers and network components.

PLANNING/COORDINATING

- Drafting of IT security policies and procedures.
- Strategy tactical planning – for servers, applications, and network infrastructure. Incumbent to review and recommend technology and/or configuration changes to achieve an optimal IT secured environment, high availability of systems, cost efficiency and data recoverability, in accordance with a multiyear tactical growth plan.

Please forward your resume quoting the competition # by online application at https://www.stclaircollege.ca/careers/apply. This link includes those who have worked for the College within 1 year of this posting. Resumes must be received prior to the closing date and time.

All active internal applicants MUST apply through the St. Clair College online application system:
https://intranet.stclaircollege.ca/human-resources/job-application-form.html

St. Clair College is committed to workplace diversity and provides accommodations to applicants with disabilities throughout our hiring process. If you require an accommodation, please contact Human Resources.

START HERE GO ANYWHERE