Job Fact Sheet Questionnaire

CAAT Job Evaluation System for Non-Bargaining Unit Employees
Ontario Colleges of Applied Arts and Technology

The Job Fact Sheet Questionnaire (JFS) is used to gather information for job evaluation purposes for the Colleges' Administrative Staff, Part-Time Support Staff, Part-Time and Sessional Academic Staff positions. Please read each section carefully before completing.

The Education and Experience sections are to be completed by the College according to the College's recruitment standards.

Upon completion by an incumbent, the JFS is reviewed and, when necessary, adjusted by the position's Manager and the Senior Manager responsible for the position. Any changes to the JFS are to be reviewed with the incumbent prior to evaluation. The JFS is then submitted to the appropriate College official for job evaluation purposes.

The JFS is not finalized until it has gone through the job evaluation process and the results have been confirmed by the College. A copy of the finalized JFS will be provided the incumbent for information purposes and as a job description.

POSITION IDENTIFICATION Date: December 1st, 2023

College:	St. Lawrence
Incumbent:	Vacant
Position Title:	Cybersecurity Operations Centre Analyst
Division/Department:	Information Technology Services
Classification:	Payband 10
Position #:	
NOC Code:	
Location/Campus:	In-Person (Tri-Campus), Hybrid, or Fully Remote
Immediate Supervisor (title):	Associate Director, Cybersecurity & IT Cloud Services

Type of Position:

☒ Administrative
☐ Part-Time Administrative
☐ Sessional Academic
☐ Part-Time Academic
☐ Part-Time Support
☐ Other

I have read and understood the contents of the Job Fact Sheet (if completed by an incumbent):

Incumbent: _____ Date: _____

Recommended by
Position's Manager: _____ Date: _____

Approved by
Senior Manager: _____ Date: _____

Job Fact Sheet Questionnaire

POSITION SUMMARY

Provide a concise description of the position by identifying its most significant responsibilities and/or accountabilities.

The **Cybersecurity Operations Centre Analyst** role is focused on ensuring St. Lawrence College **Cybersecurity Operations Centre (CSOC)** objectives are achieved, St. Lawrence College is defended from cybersecurity attacks and effective coordination of rapid responses to cybersecurity events.

An expert level knowledge and depth of experience in the field of cybersecurity operational analysis is required. Expert level knowledge of cybersecurity events, threats, vulnerabilities, incidents, protections, controls, frameworks, procedures, and leading cybersecurity practices is essential. Strong understanding of CSOC methodology is required to act as part of the St. Lawrence College CSOC team.

This position is responsible for leading cybersecurity event monitoring and analysis, threat and vulnerability analysis, incident analysis and response, as well as cybersecurity testing and validation activities within the CSOC.

As a subject matter expert for cybersecurity operational analysis, the position is responsible for continuous learning, knowledge sharing and collaboration within the St. Lawrence College community and the broader public sector cybersecurity community.

Job Fact Sheet Questionnaire

KEY DUTIES

Provide a description of the position's key duties. Estimate the percentage of time spent on each duty (to the nearest 5%). Add an extra page if necessary.

	KEY DUTIES	% OF TIME
1.	**Cybersecurity Event Monitoring & Analysis** ▪ Monitor to detect cybersecurity events. ▪ Triage and investigate cybersecurity events of concern. ▪ Determine if cybersecurity events are cybersecurity incidents.	**(40%)**
2.	**Cybersecurity Threat & Vulnerability Analysis** ▪ Detect cybersecurity threats and vulnerabilities. ▪ Analyze cybersecurity threats and vulnerabilities. ▪ Recommend cybersecurity threat and vulnerability remediation priority based on risk factors and analysis. ▪ Prepare cybersecurity threat and vulnerability reports.	**(25%)**
3.	**Cybersecurity Incident Analysis & Response** ▪ Development and cyclical review of cybersecurity incident response procedures. ▪ Triage and conduct investigatory analysis of cybersecurity incidents. ▪ Coordinate cybersecurity incidents response activities. ▪ Participate in cybersecurity incident restoration activities. ▪ Prepare cybersecurity incident reports.	**(15%)**
4.	**Cybersecurity Testing & Validation** ▪ Coordination of cybersecurity incident response simulations. ▪ Testing and validating incident response procedures. ▪ Testing and validating cybersecurity detection tools. ▪ Testing and validating cybersecurity automated protection and response tools. ▪ Testing and validating IT systems access controls. ▪ IT systems penetration testing. ▪ Prepare cybersecurity testing and validation reports.	**(10%)**
5.	**Cybersecurity Learning, Knowledge Sharing, and Community Collaboration** ▪ Develop and maintain cybersecurity operational analysis competencies and certifications. ▪ Perform research to understand cybersecurity trends and risks to prioritize cybersecurity operational improvements. ▪ Act as a Subject Matter Expert to provide advanced cybersecurity operations technical information. ▪ Actively participate in and perform cybersecurity knowledge sharing and collaboration within the St. Lawrence College community and the broader public sector cybersecurity community.	**(10%)**
	TOTAL:	**100%**

Job Fact Sheet Questionnaire

1. COMPLEXITY - JUDGEMENT (DECISION MAKING)

Complexity refers to the **variety** and relative **difficulty** of **comprehending** and **critically analyzing** the material, information, situations and/or processes upon which decisions are based.

Judgement refers to the **process** of identifying and reviewing the available options involved in decision making and then choosing the most appropriate option. Judgement involves the application of the knowledge and experience expected of an individual performing the position.

Provide up to <u>three examples</u> of the most important and difficult decisions that an incumbent is typically required to make.

a) Given a wide range of tools and technical components this person must apply expert judgement to determine the most suitable procedures to assess cybersecurity events, threats, vulnerabilities, and incident information efficiently and effectively, to prevent cybersecurity incidents and minimize the impact of cybersecurity incidents that are detected. This expert judgement considers multiple facets such as the data and IT system criticality, effectiveness of protections, effectiveness of incident response procedures, forensic preservation, escalation procedures, confidentiality and privacy considerations, communication protocols, and appropriateness for the type of cybersecurity events and incidents encountered. Apart from the initial incident response procedure planning, this person must be able to apply lateral thinking skills to identify solutions to newly identified events and incidents that may not be readily apparent and to systematically determine the root causes of specific cybersecurity issues.

b) Cybersecurity events are inherently complex. Diverse sets of event information must be correlated and analyzed to understand if a cybersecurity incident has occurred, and to identify the scope of impact and severity. Large volumes of cybersecurity event information requires implementation of automation techniques and big data analytics to successfully isolate important cybersecurity incident information. This role is responsible for designing and implementing solutions to aid with detection and analysis based on strong cybersecurity analytic skillset and experience.

c) Resolving cybersecurity incidents often involves decisions to mitigate issues with some inherent trade-offs in the impacts. Performing an assessment of the impact, recommending a course of action, and collaboration with team members is critical to understanding the complexity of the situation and to applying appropriate judgement for the response.

2. EDUCATION (to be completed by the College)

Education refers to the **minimum level** of formal education and/or the type of training or its equivalent that is required of an incumbent at the **point of hire** for the position. This may or may not match an incumbent's actual education or training.

The College is to identify the minimum level of education and/or type of training or its equivalent that is required for the position based upon the College's recruitment standards.

Non-Post Secondary

☐ Partial Secondary School

☐ Secondary School Completion

Post Secondary

☐ 1-Year Certificate

☐ 4-Year Degree

☐ 2-Year Diploma

☐ Masters Degree

☒ 3-Year Diploma/Degree

☐ Post Graduate Degree

☐ Professional Designation Specify:

☐ Other Specify:

A) Specify and describe any program speciality, certification or professional designation necessary to fulfil the requirements of the position.

- **Required certifications:**
  - **Cybersecurity & Cloud Fundamentals:**
    - (ISC)2 Certified in Cybersecurity (CC)
    - Microsoft 365 Fundamentals
    - Microsoft Azure Fundamentals
    - Microsoft Security, Compliance, Identity Fundamentals
  - **Cybersecurity & Cloud Security Analyst:**
    - (ISC)2 Certified Cloud Security Professional (CSSP)
    - (ISC)2 Systems Security Certified Practitioner (SSCP)
    - Microsoft Security Operations Analyst Associate

B) Specify and describe any special skills or type of training necessary to fulfil the requirements of the position (e.g., computer software, client service skills, conflict resolution, operating equipment).

- **Cybersecurity Incident Response Training** with strong emphasis on cybersecurity incident response coordination.
- **MITRE ATT&CK framework** and the **cyber kill chain** training or demonstrated experience.
- **NIST Cybersecurity Framework** training or demonstrated experience.
- **Cybersecurity Operations Centre (CSOC)** procedure training or demonstrated experience.
- Training to understand alerts and logs from a variety of IT Systems and cybersecurity tools (firewalls, databases, identity directories, file systems, web services, Application Programming Interfaces (APIs), Endpoint Detection and Response (EDR), Intrusion Detection / Intrusion Prevention, Multi Factor Authentication (MFA), identity federation, Active Directory, Azure Active Directory / Entra ID / Azure AD Connect / Entra ID Connect).
- Training on Security Incident and Event Management (SIEM) solutions.
- Training on Security Orchestration, Automation, and Response solutions (SOAR).
- Cybersecurity automation and programming (Python, PowerShell, Bash, or similar) training or demonstrated experience.
- Cybersecurity penetration testing training or demonstrated experience.
- Cybersecurity vulnerability analysis training or demonstrated experience.

3. EXPERIENCE (to be completed by the College)

Experience refers to the amount of **related**, **progressive** work experience required to obtain the essential techniques, skills and abilities necessary to fulfil the requirements of the job at the **point of hire** into the position. This may or may not match the incumbent's actual amount of experience.

The College is to identify the minimum amount and type of experience appropriate for the position based upon the College's recruitment requirements.

Experience required at the point of hire. Up to and including:

- ☐ no experience required
- ☐ 3 months
- ☐ 6 months
- ☐ 1 year
- ☐ 18 months
- ☐ 2 years
- ☐ 3 years
- ☐ 4 years
- ☒ 5 years
- ☐ 7 years
- ☐ 9 years
- ☐ 11 years
- ☐ 13years
- ☐ 15 years
- ☐ 17 years

Specify and describe any specialized type of work experience necessary to fulfill the requirements of the position.

- A minimum of five years of progressively responsible experience in cybersecurity operations, providing leadership in incident response, analyzing cybersecurity events, threats, vulnerabilities, incidents, testing and validation.

4. INITIATIVE - INDEPENDENCE OF ACTION

Initiative - Independence of action refers to the **amount of responsibility** inherent in a position and the **degree of freedom** that an incumbent has to **initiate** or **take action** to complete the requirements of the position. An incumbent is required to foresee activities and decisions to be made, then take the appropriate action(s) to ensure successful outcomes. This factor recognizes the established levels of authority which may restrict the incumbent's ability to initiate or take action, e.g., obtaining direction or approval from a supervisor, reliance on established procedures/methods of operation or professional practices/standards, and/or built-in-controls dictated by computer/ management systems.

A) Briefly describe up to three typical job duties/types of decisions that the incumbent is required to perform using their initiative without first having to obtain direction or approval from a supervisor.

a) The incumbent is expected to consider a diverse set of technical options related to the successful response to cybersecurity events and incidents. The incumbent must narrow the analysis to the most viable prospective options and resolution, independently of supervision.

b) The incumbent is responsible for leading the cybersecurity incident response activities within the approved parameters Cybersecurity Operations Centre (CSOC). Root cause analysis is conducted by the incumbent to determine priority improvements to avoid future incidents. The incumbent is responsible for coordination of next steps to action identified improvement opportunities.

B) Briefly describe up to three typical job duties/types of decisions that the incumbent is required to perform which required the direction or approval from a supervisor.

a) Escalation of serious cybersecurity incidents to the SLC Incident Management Team.

b) All purchases.

Give specific examples of guidelines, procedures, manuals (formal or informal), computer systems/programs that are used in performing job duties and in making decisions, e.g., Government regulations, professional or trade standards, College policies or procedures, department or program procedures, computerized/manual programs/systems and any other defined methods or procedures.

- MITRE ATT&CK Framework
- NIST Cybersecurity Framework
- OWASP Top 10
- Canadian Centre for Cybersecurity Advisories and Guidance
- Ontario Cybersecurity Higher Education Consortium (ON-CHEC) Guidance
- ON-SSOC and CanSSOC Threat Intelligence and Advisories
- Ontario Cyber Security Centre of Excellence / Cyber Security Ontario Guidance and Advisories
- OCCCIO Cybersecurity Information Advisories
- Microsoft Cybersecurity Guidance and Advisories
- Palo Alto Networks Unit 42 Guidance and Advisories
- ITIL framework for IT service management
- Application Technical Manuals and Guides
- St. Lawrence College strategic plan, business plans, policies, and procedures
- St. Lawrence College ITS strategies, standards, policies, and procedures
- St. Lawrence College cybersecurity framework, strategy, policies, standards, procedures, and controls.
- Government privacy and freedom of information legislation
- Audit requirements for information systems

5. POTENTIAL IMPACT OF DECISIONS

Potential Impact of Decisions recognizes the **potential consequences** that **errors in judgement** made by an incumbent, despite due care**,** could have on the College. Usually, the higher the level of accountability inherent in a position, the greater the potential consequences there are on the College from errors in judgement.

Give up to three examples of the typical types of errors in judgement that an incumbent could make in performing the requirements of the position. Do not describe errors which could occur as a result of poor performance, or ones that are rare or extreme. Indicate the probable effects of those errors on the College, e.g., loss of reputation of program/College, waste of resources, financial losses, injury, property damage, affects on staff, students, clients or public.

a) Errors in judgement in cybersecurity incident response or cybersecurity analysis of events, threats, vulnerabilities, and incidents could result in critical systems failures with wide-ranging consequences, privacy breaches and cybersecurity breaches. Failing to select optimal responses or to identify issues can result in missed opportunities, inefficiencies, suboptimal performance, data loss, security breaches, information exposure, organization reputational damage or significant financial impacts.

b) Failing to identify the relevant cybersecurity threats and vulnerabilities can result in severe cybersecurity breaches. Failing to identify that detected cybersecurity incidents are serious and failing to decide that they require immediate escalation of response procedures can result in very significant financial losses due to lack of appropriate incident response. The range of impact includes damage to reputation of the college, loss of revenue, financial penalties, cybersecurity insurance claims, and cybersecurity incident response costs.

6. CONTACTS AND WORKING RELATIONSHIPS

Contacts and Working Relationships refers to the **types**, **importance** and **intended outcomes** of the contacts and working relationships required by an incumbent to perform the responsibilities of a position. It also measures the skill level required to be effective in dealing with contacts and being involved in working relationships. This factor does **not** focus on the level of the contact, but on the **nature** of the contact.

Indicate by job title, with whom an incumbent is required to interact to perform the duties and responsibilities of the positions. Describe the nature, purpose and frequency of the interaction, e.g., exchanging information, teaching, conflict resolution, team consultation, counselling.

Contacts	Contacts by Job Title	Nature and Purpose of Contact	Frequency of Contact	
Internal to the College:			Occasional	Frequent
Internal to the college, e.g. students, staff, senior management, colleagues.	Directors of All College Areas	Gathering project and IT solutions requirements		X
	Deans and Associate Deans	Gathering project and IT solutions requirements		X
	Functional Support Staff	Gathering project and IT solutions requirements, directing project activities, coordinating IT systems support issue resolution		X
	ITS Senior Management (Directors, CISO, CIO)	Gathering project and IT solutions requirements, reporting on project status, seeking approval for significant project changes, seeking approval for significant changes to IT systems or availability of IT systems availability, coordinating IT systems support issue resolution		X
	ITS Technical Staff	Gathering project and IT solutions requirements, directing project activities, coordinating IT systems support issue resolution		X
	College Executive Team	Gathering project and IT solutions requirements	X	

Job Fact Sheet Questionnaire

External to the College:			Occasional	Frequent
External to the college, e.g. suppliers, advisory committees, staff at other colleges, government, public/private sector.	Application Vendors and Contracted Service Providers	Managing project activities and contracted services, coordinating IT systems support issue resolution		X
	Contracted Consultants	Managing the delivery of specialized knowledge or expertise		X

Occasional (O) **Contacts are made once in a while over a period of time.**
Frequent (F) **Contacts are made repeatedly and often over a period of time.**

7a. CHARACTER OF SUPERVISION/FUNCTIONAL GUIDANCE

Character of Supervision identifies the **degree and type** of supervisory responsibility in a position or the nature of functional/program supervision, technical direction or advice involved in staff relationships.

(√) Check the applicable box(es) to describe the type of supervisory responsibility required by an incumbent in the position:

- ☐ Not responsible for supervising or providing guidance to anyone.
- ☒ Provides technical and/or functional guidance to staff and/or students.
- ☐ Instructs students and supervises various learning environments.
- ☒ Assigns and checks work of others doing similar work.
- ☒ Supervises a work group. Assigns work to be done, methods to be used, and is responsible for the work performed by the group.
- ☐ Manages the staff and operations of a program area/department.*****
- ☐ Manages the staff and operations of a division/major department.*****
- ☐ Manages the staff and operations of several divisions/major departments.*****
- ☐ Acts as a consultant to College management.
- ☐ Other e.g., counselling, coaching. Please specify:
  -

***** Includes management responsibilities for hiring, assignment of duties and work to be performed, performance management, and recommending the termination of staff.

Specify staff (by title) or groups who are supervised/given functional guidance by an incumbent.

- Various cross-functional staff that are involved in cybersecurity operations or cybersecurity incident response. The incumbent must manage their activities in relation to relevant cybersecurity operational priorities, ITS procedures and approved commitment of time by the staff members' immediate supervisors.

7b. SPAN OF CONTROL

Span of Control is complementary to **Character of Supervision/Functional Guidance**. Span of Control refers to the **total number of staff** for which the position has supervisory responsibility, (i.e., subordinates, plus all staff reporting to these subordinates).

Enter the total number of full time and full time equivalent staff reporting through to the position. Also identify the number of staff for whom the position has indirect responsibility (contract for service), if applicable.

Type of Staff	Number of Staff
Full-Time Staff	0
Non Full Time Staff (FTE) *	0
Contract for Service **	0
Total:	0

* Full Time Equivalency (FTE) conversions for non full time staff are as follows:

Academic Staff

Identify the total average annual teaching hours taught by all non full time teachers (part-time, partial load and sessional) for which the position is accountable and divide by 648 hours for post secondary teachers and 760 hours for non-post secondary teachers.

Support Staff

Identify the total average annual hours worked by part-time support staff for which the position is accountable and divide by 1820 hours.

Administrative Staff

Identify the total average annual hours worked by non full time administrative staff for which the position is accountable and divide by 1820 hours.

** Contract for Services

When considering “contracts for services,” review the nature of the contractual arrangements to determine the degree of “supervisory” responsibility the position has for contract employees. This could range from “no credit for supervising staff” when the contracting company takes full responsibility for all staffing issues to “prorated credit for supervising staff” when the position is required to handle the initial step(s) when contract staffing issues arise.

8. PHYSICAL AND SENSORY DEMANDS

Physical/Sensory Demands considers the **degree** and **severity** of exertion associated with the position. The factor considers the intensity and severity of the physical effort rather than the strength or energy needed to perform the task. It also considers the sensory attention required by the job as well as the frequency of that effort and the length of time spent on tasks that cause sensory fatigue.

Identify the types of physical and/or sensory demands that are required by an incumbent. Indicate the frequency of the physical demands as well as the frequency and duration of the sensory demands. Use the frequency and duration definitions following the tables to assist with the descriptions.

PHYSICAL DEMANDS

Describe the types of activities and provide examples that demonstrate the physical effort that is required in the position on a regular basis, i.e., sitting, standing, walking, climbing, lifting and/or carrying light, medium or heavy objects, pushing, pulling, working in an awkward position or maintaining one position for a long period of time.

Types of Activities that Demonstrate Physical Effort Required	**Frequency** (note definitions below)				
	Occasional	**Moderate**	**Considerable**	**Extended**	**Continuous**
Sitting at computer station for data entry, system testing, updates, etc.			X		
Normal computerized office environment – standing, walking, bending to retrieve files, using office equipment, etc.					X

SENSORY DEMANDS

Describe the types of activities and provide examples that demonstrate the sensory effort that is required in the position on a concentrated basis, i.e., reading information/data without interruption, inputting data, report writing, operating a computer or calculator, fine electrical or mechanical work, taking minutes of meetings, counselling, tasting, smelling etc.

Types of Activities that Demonstrate Sensory Effort Required	**Frequency** (note definitions below)					**Duration**
	Occasional	**Moderate**	**Considerable**	**Extended**	**Continuous**	**Short Intermediate or Long**
Performing analysis of IT systems operations and support issue resolution				X		L
Concentrated development of project management plans and schedules using a variety of computer applications				X		L
Preparing status reports, proposals, and presentations				X		L

Job Fact Sheet Questionnaire

Types of Activities that Demonstrate Sensory Effort Required	Frequency (note definitions below)					Duration
	Occasional	Moderate	Considerable	Extended	Continuous	Short Intermediate or Long
Email communication with project team members, stakeholders and ITS staff			X			S

Job Fact Sheet Questionnaire

FREQUENCY:

Occasional:	Occurs once in a while, sporadically.
Moderate:	Occurs on a regular, ongoing basis for up to a quarter of the work period.
Considerable:	Occurs on a regular, ongoing basis for up to a half of the work period.
Extended:	Occurs on a regular, ongoing basis for up to three-quarters of the work period.
Continuous:	Occurs on a regular, ongoing basis throughout the entire work period except for regulated breaks.

DURATION:

Short:	Up to one hour at a time without the opportunity to change to another task or take a break.
Intermediate:	More than one hour and up to two hours at a time without the opportunity to change to another task or take a break.
Long:	More than two hours at a time without the opportunity to change to another task or take a break.

9. WORKING CONDITIONS

Working Conditions considers the frequency and type of exposure to undesirable, disagreeable environmental conditions or hazards, under which the work is performed.
Describe any unpleasant environmental conditions and work hazards that the incumbent is exposed to during the performance of the job.

Environment

Describe the types of activities and provide examples that demonstrate exposure to unpleasant environmental conditions in the day-to-day activities that are required in the job on a regular basis, e.g., exposure to dirt, chemical substances, grease, extreme temperatures, odours, noise, travel, verbal abuse, body fluid, etc. Indicate the activity as well as the frequency of exposure to undesirable working conditions.

Note on Travel: St. Lawrence College has adopted the following guidelines for travel. From the list below, please indicate which category best describes the travel required for the position.

1. *Local travel on a regular basis up to 2 times per week.*
   Out-of-town travel on a regular basis 1 – 2 times per month.
2. *Local travel on a regular basis more than 2 times per week.*
   Out-of-town travel 2 – 8 times per month.
3. *Out-of-town travel on a regular basis more than 8 times per month.*

Types of Activities That Involve Job Related Unpleasant Environmental Conditions. Include travel requirements (if any).	**Frequency** (note definitions below)		
	Occasional	**Frequent**	**Continuous**
Travel to attend project meetings (Tri-campus)	X		

Hazards

Describe the types of activities and provide examples that demonstrate the hazards in the day-to-day activities that are required in the job on a regular basis, e.g. chemical substance, electrical shocks, acids, noise, exposure to infectious disease, violence, body fluids, etc. Indicate the activity as well as the frequency of exposure to hazards.

Types of Activities That Involve Job Related Hazards	**Frequency** (note definitions below)		
	Occasional	**Frequent**	**Continuous**
Not applicable.			

Frequency:

Occasional	Occurs once in a while, sporadically.
Frequent	Occurs regularly throughout the work period.
Continuous	Occurs regularly, on an ongoing basis, throughout most of the work period.