STRENGTH

PEACE

UNITY

Mohawk Council of Kahnawake

P.O. Box 720
Kahnawake Mohawk Territory J0L 1B0

Tsi Nikaio'tenhseró:tens Ne Onkweshón:'a Rotiió'tens

HUMAN RESOURCES UNIT

Tel.: (450)632-7500
Fax: (450)638-5958
Website: www.kahnawake.com

INTERNAL/EXTERNAL

JOB OPPORTUNITY

POSITION:	**Security Administrator, Information Management**
DURATION:	Indeterminate, Full-Time Nine (9) Month Probation Period
DESCRIPTION:	See Attached Job Description
SALARY:	$1,267.13 to $1,710.75 Per Week
Hours of Operation	8:30 a.m. to 4:00 p.m.
Hours per week	37.5 hours per week
DEADLINE FOR APPLICATION:	**Monday, May 13, 2024 - 4:00 p.m.**
REQUIREMENTS:	**ALL REQUIRED DOCUMENTS MUST BE SUBMITTED BEFORE THE DEADLINE FOR YOUR APPLICATION TO BE CONSIDERED**

- ✓ Applicant checklist
- ✓ Letter of intent
- ✓ Resume

APPLICATION: Please address your application to Dawn Stacey, Manager of Recruitment & Staffing. Forward your complete application via e-mail only to: Applications@mck.ca

NOTE: All forms and requirements are listed on our website: www.kahnawake.com/jobs

- **Please ensure complete applications are submitted as requested. Incomplete applications may not be considered.**
- **Only candidates selected for an interview will be contacted.**
- **Preference will be given to Aboriginal candidates.**

STRENGTH

PEACE

UNITY

Mohawk Council of Kahnawake

P.O. Box 720
Kahnawake Mohawk Territory J0L 1B0
Tsi Nikaio'tenhseró:tens Ne Onkweshón:'a Rotiió'tens
HUMAN RESOURCES UNIT

Tel.: (450)632-7500
Fax: (450)638-5958
Website: www.kahnawake.com

Job Title:	Security Administrator
Division:	Information Management
Reports To:	Director of Information Management
Name of Incumbent:	TBD

Purpose: To ensure the secure operation of the in-house computer systems, servers, and network connections. This includes checking server and firewall logs, scrutinizing network traffic, establishing and updating virus scans, and troubleshooting.

To analyze and resolve security breaches and vulnerability issues in a timely and accurate fashion, and conduct user activity audits where required.

Cultural Identity Attributes: A professional, technically proficient individual with a strong problem-solving orientation and commitment to customer service and continuous learning. Is adaptable, collaborative and a strong communicator who adheres to policies and respects confidentiality.

Roles & Responsibilities:

Strategy & Planning

- Develop, implement, maintain, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices.
- Design and implement disaster recovery plans for operating systems, databases, networks, servers, and software applications.
- Assess the need for any security reconfigurations (minor or significant) and execute them if required.
- Keep current with emerging security alerts and issues.
- Conduct research on emerging products, services, protocols, and standards in support of security enhancement and development efforts.
- Work in close collaboration with the IM Team members.

Acquisition & Deployment

- Interact and negotiate with vendors, outsourcers, and contractors to obtain protection services and products.
- Recommend, schedule, and perform security improvements, upgrades, and/or purchases.

Operational Management

- Deploy, manage, and maintain all security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software.
- Administer and maintain end user accounts, permissions, and access rights.
- Manage connection security for local area networks, the company web site, the company intranet, and e-mail communications.
- Manage and ensure the security of databases and data transferred both internally and externally.
- Design, perform, and/or oversee penetration testing of all systems to identify system vulnerabilities.
- Design, implement, and report on security system and end-user activity audits.
- Monitor server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interpret activity and make recommendations for resolution.
- Recommend, schedule (where appropriate), and apply fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach.
- Download and test new security software and/or technologies.
- Provide Security analysis for arms reach community entities and provides recommendations.
- Provide on-call security support to end-users.
- Manage and/or provide guidance to junior members of the team.

The statements herein reflect general details to describe the principle functions for this job and should not be considered an all-inclusive listing of work requirements. Individuals may perform other duties or be assigned projects associated with these responsibilities as directed by their immediate supervisor.

Decision-Making Authority:

- Determines best methodology and approach for new initiatives/projects.
- Decides on Security policies approaches and Security technology.
- Determines the need for any security reconfigurations (minor or significant).

Accountability:

- Accountable to the Director of Information Management for reports and regular updates.
- To ensure the secure operation of the in-house computer systems, servers, and network connections.
- To ensure the safety and security of MCK data and digital information.
- To resolve security breaches and vulnerability issues in a timely and accurate fashion.
- Conduct business with internal and external clients in a tactful, discreet and courteous manner.
- Maintain confidentiality.

- Adhere to the MCK Administration Manual-Personnel Policy and Kanien'kéha Language initiatives.

Education & Experience:

- University Degree or a College Diploma in the field of computer science and two (2) years of relevant work experience.
- Certification in any of the following: CEH; CISSP; CISA; Security+ CISM; GSEC; SSCP or CASP are considered an asset.

Knowledge, Skills, Abilities, and Other Attributes:

- Broad hands-on knowledge of firewalls, intrusion detection systems, anti-virus software, data encryption, and other industry-standard techniques and practices.
- In-depth technical knowledge of network, PC, and platform operating systems, including both Windows and Unix.
- Working technical knowledge of current systems software, protocols, and standards, including ISO, SOC ITIL.
- Strong knowledge of TCP/IP and network administration/protocols.
- Hands-on experience with devices such as hubs, switches, and routers.
- Knowledge of applicable practices and laws relating to data privacy and protection.
- Knowledge of law enforcement practices and procedures, such as privacy laws.
- Intuition and keen instincts to pre-empt attacks.
- High level of analytical and problem-solving abilities.
- Ability to conduct research into security issues and products as required.
- Strong understanding of the organization's goals and objectives.
- Strong interpersonal, oral and written communication skills.
- Highly self-motivated and directed.
- Strong organizational skills.
- Excellent attention to detail.
- Ability to present ideas in user-friendly language.
- Ability to effectively prioritize and execute tasks in a high-pressure environment.
- Able to work in a team-oriented, collaborative environment.
- Ability to communicate in the Kanien'kéha and French languages is an asset.
- The willingness to learn the Kanien'kéha language is required.

Working Environment:

- Five-day work week in an office environment.
- Occasional overtime or on-call work may be required.

- Occasional travel.
- Moderate to high stress and productivity pressure.
- Lifting and transporting of moderately heavy objects, such as servers and peripherals.

Competencies:

Self - Management	**Client & Team Relations**	**Quality Decision Making**	**Professional Capacity**	**Communication**	
Intermediate	Intermediate	Intermediate	Core	Intermediate	
Adaptability	**Planning and Organizing**	**Leadership**	**Language & Culture**		
Intermediate	Intermediate	Core	Core		

Commitment Statement:

I serve my community with its best interest in mind by supporting and encouraging creative, critical, and resourceful thinking, accepting and nurturing new ideas and approaches, and demonstrating my dedication and integrity through my efforts, actions, and words. I am part of a team that is empowered to take initiative in an interactive working environment.

Signatures:

Employee's Signature: ____

Date: ____

Supervisor's Signature:____

Date: ____