We are looking for a

GLOBAL INFORMATION SECURITY MANAGER

The company :

EJ is the world leader in the design, manufacture and distribution of access solutions for water, sewer, drainage, telecommunications and utility networks worldwide. Our technical expertise allows us to provide innovative solutions for infrastructure projects in more than 150 countries around the world. We are a family-owned company that spans 5 continents, promoting innovation, quality and a commitment to customer service. Our commercial presence worldwide includes 50 sales offices, 10 manufacturing facilities and multiple research and development centers.

We are committed to create an environment that promotes diversity and to be an equal opportunity employer.

Our People are our core strength. Faithful, qualified and experts in their field, our employees come from diverse backgrounds but are united by their skills, their professionalism and their team spirit.
We are attentive to the evolution of the skills of our employees, their loyalty is a priority. We promote internal mobility, measure employee performance through an annual appraisal system, and support skills development through the implementation of training through various systems.

https://www.ejco.com/

Mission :

The global information security manager (ISM) is a critical member of the Information Security and Privacy Department (ISPD). This position is an interface between the CIO's strategic and process-based security activities and the work of the technology focused analysts, engineers and architects in the IT organization. This role provides strategic, architectural and operational support of the global information security program; and is considered a global technical resource for region IT Departments to assure the consistent implementation of global security controls.

The Global Information Security Manager is also responsible to help monitor EJ regional information systems for access control violations/intrusion detection, cybersecurity problems and malware issues, as well as assist with recovery from access control violations, malware attacks and cybersecurity attacks.

Essential Duties and Responsibilities : include the following. Other duties may be assigned.

- Promotes safety awareness, accident prevention, and employee involvement with regard to a safe work environment. Ensures employees have an understanding of the safety expectations of the organization.
- Promotes the company culture, the mission and vision, and the core values of the company.
- Must be able to translate the IT-risk based requirements and constraints of the business into technical control requirements and specifications, as well as develop metrics for ongoing performance and management.
- Coordinates the IT organization's technical activities to implement and manage the global security infrastructure and provides regular status and service-level reports to management.

Strategic Support

- Administer and propose changes to the Company Information Security and Privacy Program. Major components of the program include policies, security and privacy awareness training, technical system controls and audits.
- Work with the CIO and regional IT Departments to identify areas of high security and privacy risk and propose appropriate policies, training and controls to the Information Security and Privacy Department.
- Identify opportunities to both improve and simplify global information technology security management, including reducing the number of and variety of dissimilar technology platforms.

Architectural/Engineering Support

- Work with the regional IT Departments to assure that security measures are built into all internal, interfaced and third-party systems housing confidential/private data.
- Document where security policies are not 100% attainable. Work with the regional IT departments to manage these exceptions and create plans and processes to eliminate the exceptions where appropriate.
- Work with the regional IT Departments to assure proper implementation of security controls, and schedule audits where compliance is suspect.
- Conduct audits of security policies and vulnerability tests of security controls and make recommendations for improvements. Validate that each region has properly implemented the security program.
- Work with global IT teams on disaster recovery and resiliency planning and test.
- Research, evaluate, design, test, recommend or plan the implementation of new information security hardware and software, and analyze its impact on the existing environments; provide the technical and managerial expertise for the administration of security tools.
- Provide assistance to the regional IT Departments with the configuration and operation of the various information technology system for a highly secure environment to meet all global security and privacy legal compliance requirements.

Operational Support

- Monitor the company execution of the security and privacy program to validate the program is implemented and processes are completed as outlined and scheduled in the security policies; or recommend policy changes.
- Proactively monitor global system reports for access control violations/intrusion detection, cybersecurity problems and malware issues.
- Actively work with regions on complex incident detection, troubleshooting, resolution and recovery, and reporting from access control violations, malware attacks and cybersecurity attacks.
- Maintain a knowledgebase for information security topics, such as security advisories and alerts for IT and the general employee population.
- Ensure audit trails, system logs and other monitoring data sources are reviewed periodically and are in compliance with policies.

Security Liaison

- Assist personnel and IT Departments in understanding and responding to security issues and security audit concerns.
- Work with various global department leaders, including IT, HR, plant IT and Finance, to educate them on security risks and necessary controls and to identify new risks and appropriate controls.
- Monitor all security incidents to validate that each region has completed all steps for all incidents, including post-incident reviews and follow-up steps. Actively participate in incidents to assure that lessons learned from other incidents are shared throughout the organization and are properly documented for global sharing.
- Keep abreast of security alerts by information system vendors, government agencies, professional associations and other organizations as needed, communicate the alerts as appropriate, and make recommendations of precautionary steps.
- Keep abreast of global information security and privacy regulatory changes and make appropriate policy, training and control recommendations to the ISPD to meet legal requirements.

- Work with the CIO, IT Departments and ISPD to develop, report and monitor a security performance dashboard to be used by the ISPD and global IT regions.
- Be the global consolidator and disseminator of technical expertise on security capabilities of various security and privacy technologies to assure consistent global implementation of security controls.

Qualifications :
To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Education and/or Experience :
Bachelor's degree (B.A. or B.S.) from a four-year college or university, several years of related IT experience, multiple years' experience in an IT security and infrastructure role and security certifications desired.

Other Skills and Abilities :
- Spoken and written English language proficiency required
- Spoken and written French language proficiency desired
- Expertise in leading project teams and developing and managing projects
- Ability to collaborate and facilitate action with different IT organizations who do not directly report to this position
- Ability to clearly present ideas to EJ Leaders or other IT Department members
- Strong analytical skills
- Excellent verbal, written, and interpersonal communication skills

Physical Demands :
The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is regularly required to sit and use hands to finger, handle, or feel. The employee frequently is required to talk or hear. The employee is occasionally required to stand; walk; reach with hands and arms; climb or balance; and stoop, kneel, crouch, or crawl. The employee must occasionally lift and/or move up to 50 pounds. Specific vision abilities required by this job include close vision, color vision, and ability to adjust focus.

Work Environment :
The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is occasionally exposed to moving mechanical parts, extreme heat, and risk of electrical shock. The noise level in the work environment is usually moderate, although there is an occasional need to work in the manufacturing environment, where noise levels are increased.

Travel :
Overnight and international travel required.

Please send cover letter and resume to :

EJ Picardie
Direction des Ressources Humaines
drh@ejco.com