Rail Baltica
Coordinated by RB Rail

Vacancy

IT SECURITY EXPERT

Rail Baltica is the largest Baltic transport infrastructure project that will create the North – East economic corridor. It will be an electrified, high speed railway line with modern infrastructure for passenger and freight services, ensuring environmentally friendly and fast transportation from Tallinn to the Lithuanian-Polish border. Rail Baltica will connect the Baltic States with Central and Western Europe. The project is largely co-financed by the European Union. It must be well-governed, with clear financial flows and procurement systems. RB Rail AS is looking for a new enthusiastic **COLLEAGUE** to join our growing team in a position of **IT SECURITY EXPERT.**

Our ambition is to plan, monitor and control the delivery the new best-in-class, innovative, environmentally friendly railway infrastructure with cost competitive technical solution in the region to improve the long-term well-being of the society of the Baltic States and European community. We plan, develop and manage all technical aspects of entire Rail Baltica project to achieve cross-border interoperability. RB Rail AS is the three Baltic States' joint venture, it was established in October 2014 and is registered in Latvia. Main business of the joint venture is the design, construction and marketing of the railway. RB Rail acts as a main coordinator of the project.

JOB PURPOSE:

IT Security Expert is responsible for development, implementation, monitoring, and maintenance of the information and cyber security program, including identifying critical systems and critical digital assets, addressing cyber security controls for each critical digital asset, and maintaining cyber security attack mitigation and incident response capability.

REQUIREMENTS

- Professional degree in Computer Science, Information Systems, Cyber engineering or equivalent (Master's degree is preferable)
- 5+ years of varied information technology experience is required
- 5+ years of direct experience in information/cyber security-related duties is required
- 3+ experience in developing security concepts/strategies, security planning and organization. Proficiency to develop and draft internal regulatory enactments – policies, regulation, plans, guidelines etc.
- Applicable experience includes, but is not limited to, cyber security, computer and networking infrastructure, operating systems, application software development, project management, regulatory compliance, risk management, and providing training
- Good knowledge to navigate in areas of Latvian law related to national security, security of IT critical infrastructure, security of IT, NIS Directive and related national legislation, as well as GDPR. Ability to orientate in the EU requirements of information security management and information and communication technology (ICT) regulations and international standards, as well as in the generally accepted practice in the field of information security
- Ability to develop information security management structure/architecture, incl. to describe the roles, duties, responsibilities of the responsible persons
- Experience in information security, specifically with penetration testing, intrusion detection, incident response or digital forensics
- Proficiency in information/cyber security risk management
- Ability to identify information and cyber security vulnerabilities, threats, assess and calculate the impact of the threat, determine the probability
- Experience working within a international team setting
- Advanced certifications such as SANS GIAC/GCIA/GCIH, CISSP, CISA, CISM or equivalent will be considered advantageous
- Advanced understanding of hardware and software systems is required
- Experience to maintain confidentiality in regard to information processed, stored, or accessed by the systems is required
- Advanced understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, defence-in-depth and common security elements
- The ability to manage multiple concurrent projects and to reason analytically is required
- The ability to work with and train people possessing differing levels of technical knowledge is required
- Proficiency in writing technical specifications are required
- Proficiency in incident investigations
- Ability to orientate in the company's business continuity processes and ensure the planning and monitoring of information system renewal activities
- Ability to use logic and reasoning to identify the strengths and weaknesses of IT systems
- Ability to organize, plan and control effectively one's work, set the priorities independently and planning the work according to them
- Excellent Latvian language skills
- Good command of spoken and written English
- High ethical standards, honesty, and impeccable reputation
- Experience in the Transport industry will also be advantageous

RESPONSIBILITIES

- Creates vision for IT security strategies, both short-term and long-term
- Develop and direct an ongoing, proactive risk assessment program for IT infrastructure
- Communicates risks and recommendations to mitigate risks to the direct manager and the senior management
- Organise the confidentiality, integrity, and availability of information resources by creating and maintaining enforceable policies, regulations and supporting processes, and ensuring compliance with regulatory requirements
- Oversees all ongoing activities related to the development, implementation, and maintenance of the Company's IT security policies and procedures by ensuring these policies and procedures encompass the overall security of IT infrastructure
- Chairs the IT Security Committee (ITSC) and coordinates the activities of ITSC so that security decisions do not interrupt business processes while maintaining the confidentiality, integrity, and availability of information resources
- Acts proactively and advise IT department to prevent potential disaster situations by ensuring that proper protections are in place, such as intrusion detection and prevention systems, firewalls, and effective physical safeguards, and contribute for the availability of ensuring a business continuity/disaster recovery plan, other IT security issues
- Evaluates security incidents and determines what response, if any, is needed and coordinates IT department responses
- Develops information security awareness training and education programs to present them to employees, and participates in local, regional, and national awareness and education events, as appropriate
- Organize developing design, construction and railway systems and IT infrastructure architecture and cyber security solutions
- Recognizes problems by identifying unusual activities; running counteractive protocols; reporting violations
- Act as internal expert on matters relating to intrusion detection and incident response
- Lead investigations into network intrusions and other cyber security breaches. Provide a coordinated response to complex cyber-attacks that threaten assets, intellectual property, and computer systems
- Contribute to the development of new defensive systems and protocols and improvement of security monitoring and incident response processes and solutions by assessing current situation; evaluating trends; anticipating requirements
- Determines security violations and inefficiencies by conducting periodic audits
- Upgrade systems by implementing and maintaining security controls
- Keep users informed by preparing performance reports

OFFICE LOCATION

Full time located in Riga, Latvia

SALARY

Starting from 4000 EUR (before taxes).

APPLICATION PROCESS

If you are willing to be a part of the challenging and unique project, and your experience and personality match the position's requirements, please, send your CV and motivation letter in English with the subject "IT SECURITY EXPERT" to RB Rail AS recruitment partners SIA "Recruitment Latvia": rbrail@cvor.lv by 11 April 2021.

By submitting this application (CV, motivation letter, etc) the applicant provides the authorisation for the processing of personal data by RB Rail AS ("Controller") and SIA "Recruitment Latvia", Reg. No 40003955719, as its respective recruitment partners. The personal data indicated in the application documents will be processed for the purposes of the recruitment and hiring processes only as is legally permissible under Art. 6(1)(f) of Regulation (EU) 2016/679 (General Data Protection Regulation)

Co-financed by the Connecting Europe Facility of the European Union