Job Description

Information Security Specialist

Position: Information Security Specialist

Reports to: CIO

Supervision of: N/A

Duty station: Norway/Germany/in any NRC office

Travel: Low, up to 10% depending on workplan

Project number: XXX

Duration and type of contract: Permanent

All NRC employees are expected to work in accordance with the organisation’s core values: dedication, innovation, inclusivity and accountability. These attitudes and beliefs shall guide our actions and relationships.

**Background:**

NRC’s global strategic plan for 2022 - 2025 includes Digital Transformation as a strategic enabler for the organisation and a key element in expanding the reach of our assistance towards the 2030 ambition. To do so, NRC is increasingly adopting digital solutions to drive internal efficiencies as well as provide digital services to the people it serves. Key to all this will be NRC’s ability to secure systems, applications and the data these will process, to ensure privacy, confidentiality and avoid causing digital harm.

As the Information Security Specialist, you will be working in the global ICT Development Section, alongside the Information Security Risk Management Advisor, ICT operations, infrastructure and development teams to improve our digital security set-up and practices.

1. **Role and responsibilities**

Generic responsibilities

1. Contribute to uphold confidentiality, integrity and availability of information and systems at NRC;
2. Coordinate and collaborate across the ICT Development Section and with other parts of the organisation on dependencies and opportunities related to information security;
3. Ensure that information security is integrated in all digital initiatives, providing guidance to project managers and service providers;
4. Contribute to the development and implementation of policies, frameworks and procedures related to information security;
5. Innovate and experiment, including capturing smart failure (failure that generates learning);
6. Capture learning and disseminate to the unit, section and organisation through adequate documentation and/or ad hoc presentations;
7. Contribute to business continuity and disaster recovery plans;
8. Raise staff awareness and build staff capacity on mitigation of information security risks;
9. Provide inputs for budgetary planning related to information security;

Specific Responsibilities:

1. Contribute to the establishment of critical elements of an Information Security Management System in line with the standards such as the CIS or ISO27001 frameworks;
2. Assist in development and implementation of CIS 20 controls across the organization, for both hardware and software;
3. Develop, maintain, and present IT security education, awareness, and training for all members of the organization as appropriate;
4. Work in tandem with NRC’s developer team and external developer consultants (code/configuration flaws) to ensure we are addressing security concerns in our architecture and development efforts. Identify and develop tools to improve this process.
5. Provide cyber-security input, advice and reviews on any digital solution development and implementation;
6. Design, implement new, and review existing, IT security measures and controls from Information security perspective and guide ICT team to correct the identified gaps;
7. Contribute to testing, setting up and monitoring a SIEM solution on prioritised components;
8. Manage periodic security audits and vulnerability and threat assessments and direct responses to network or system intrusions;
9. Assess any identified information security risks, proposed remedial actions and keep the track of these;
10. Handle serious IT operational incidents or security breaches in accordance with ITIL process, including being responsible for assembling solution teams consisting of internal resources and suppliers, as well as leading these.
11. Ensure that processes are documented and communicated in language that is relevant and understandable to non-technical audiences

Critical interfaces

By interfaces, NRC means processes and projects that are interlinked with other departments/units or persons. Relevant interfaces for this position are:

* ICT Support and Operations, Digital Transformation and Centre of Excellence for Data and Analytics teams
* Focal points of other digital initiatives (Finance, M&E, HR, Logistics, Private fundraising, etc.)
* Project managers and technical owners for systems and or applications at NRC
* Data Protection and Information Security Advisers
* Suppliers, consultants, and other external service providers
* Peers from other organisations working on similar solutions, particularly in the NetHope community
1. **Competencies**

Competencies are important for the employee and the organisation to deliver the desired results. They are relevant for all staff and are divided into the following two categories:

1. Professional competencies

These are skills, knowledge and experience that are important for effective performance.

**Generic professional competencies for this position**:

* Bachelor’s degree in computer science, software engineering, or related subjects, or demonstrable expertise in the field.
* Background in Product Security and/or Application Security teams with enterprise and/or cloud applications
* Strong knowledge of IT service management software including ITIL
* Knowledge of information security standards rules, benchmarks and regulations related to information security and data confidentiality (ISO27001, GDPR, CIS-Azure etc.)
* Understanding of possible attack activities such as network probing/ scanning, DDOS, malicious code activity, etc.
* Understanding of common network devices such as firewall, routers, switches.
* Understanding in system security architecture and security solutions
* Experience and overview with Azure, AWS, or other cloud platform providers
* Experience with Docker and Kubernetes is good to have.
* Certification such as Certified Information Security Manager (CISM), is Certified Information Security Auditor (CISA) are an advantage.
* Excellent interpersonal and communication skills, comfortable working with a geographically distributed team, and can easily work with non-technical colleagues.
* Fluency in written and spoken English. Other languages are an asset.

**Context/Specific skills, knowledge and experience**:

* Knowledge of cloud security concepts, technologies, and best practices, including but not limited to, automation frameworks, securing containers and container orchestration frameworks, Active Directory, LDAP, Federated SSO, One-Time Password (OTP) technology, SSL, encryption, IDS/IPS, SIEM, malware detection, forensics in a cloud environment, network and web app firewalls.
* Skills in the use of vulnerability assessment and penetration testing tools.
* Able to write sufficient and easy-to-understand technical documentation.
* Comfortable with presenting technical information to a non-technical audience.
* Knowledge of cloud-based technologies (e.g O365, Azure, Kubernetes, Docker and OKTA Authentication tool) is considered a plus
* Great team player to support other team members and ready to share existing workloads.

2. Behavioral competencies

* **Analysing:** Understands and sees problems from different angles; able to break down complex problems and connect the dots; considers contextual caveats and risks.
* **Planning and delivering results:** Take initiative and see things through to completion; anticipate problems and solve them, can operate with little to no direction.
* **Coping with change:** Adopts a flexible and responsive mindset; comfortable with uncertainty; can adapt plans quickly.
* **Working with people:** A team player by nature; able to build bridges across silos; defaults to sharing and supporting colleagues in achieving their goals; focuses on solutions rather than obstacles.
1. **Performance Management**

The employee will be accountable for the responsibilities and the competencies, in accordance with the NRC Performance Management Manual. The following documents will be used for performance reviews:

* The Job Description
* Work and Professional Development Plan
* The Mid-term/End-of-trial Period Performance Review Template
* The End-term Performance Review Template
* The NRC Competency Framework