National Student Financial Aid Scheme

Job Specification & Recruiting Profile of Vacancy

25 August 2023

The following vacancy exists at NSFAS in Cape Town.

Position	Cyber Security Analyst	**Type & Grade**	Permanent – C5
Vacancy No	20 of 2023/24	**Department & Unit**	ICT -Technology

POSITION OVERVIEW:

The main purpose of the job is to protect NSFAS's information technology (IT) systems, networks, and data from potential cyber threats and attacks. This position will be required to perform strategic and tactical cybersecurity functions. Specifically related to researching, auditing and reporting in cyber security, assessing Information Security controls, Business Continuity Planning, resolving audit findings and supporting information security projects.

RESPONSIBILITIES:

Policy, Systems & Procedure Development

- To implement the NSFAS cloud systems processes in line with policy requirements
- To service and resolve all queries that emanate from the business relating to cloud systems.

- To implement and maintain all security policies relating to cloud systems.

Core Objectives Implementation

- Threat Monitoring and Incident Response: Monitoring IT systems and networks for potential cybersecurity threats, detecting and responding to security incidents in a timely manner, investigating security breaches, and taking appropriate actions to mitigate risks.
- Vulnerability Assessment and Penetration Testing: Conducting vulnerability assessments and penetration testing to identify potential weaknesses in IT systems, networks, and applications, and recommend appropriate remediation measures to address identified vulnerabilities.
- Security Operations: Implementing and managing security tools and technologies such as firewalls, intrusion detection and prevention systems (IDPS), security information and event management (SIEM) systems, antivirus software, and other security controls to protect against cyber threats.
- Security Incident Analysis: Analyzing security events and logs to identify potential security incidents, investigating security alerts, and determining the root cause of security incidents.
- Security Policy and Procedure Development: Developing and implementing security policies, standards, procedures, and guidelines to ensure compliance with industry best practices, regulatory requirements, and organizational security requirements.
- Security Risk Assessment: Conduct risk assessments to identify and evaluate potential security risks and recommend appropriate risk mitigation measures.
- Security Awareness and Training: Conducting security awareness and training programs for employees, educating them about cybersecurity best practices, and promoting a culture of security awareness across the organization.
- Security Incident Reporting and Documentation: Preparing and maintaining documentation related to security incidents, including incident reports, investigation findings, and recommendations for improvement.
- Cyber Threat Intelligence: Staying updated with the latest cybersecurity threats, vulnerabilities, and trends, and leveraging cyber threat intelligence to proactively identify and address potential security risks.
- Collaboration and Coordination: Collaborating with other IT and security teams, as well as other stakeholders in the organization, to ensure a coordinated and effective response to cybersecurity

incidents and to implement appropriate security measures.

- Compliance and Audits: Ensuring compliance with relevant cybersecurity regulations, standards, and frameworks, and supporting internal and external audits related to information security.
- Incident Response Planning: Developing and maintaining incident response plans, including defining roles and responsibilities, establishing communication channels, and documenting response procedures

Stakeholder Management & Relationships

- To provide development support as per request within the agreed SLA.
- To ensure no rejections from the requestor.
- To provide UAT support as per request within the agreed SLA.
- To receive stakeholder queries.
- To resolve stakeholder queries within the given time frame.
- To produce timeous and accurate reports.
- To run the tools that verify the efficiency of systems and tunes if necessary (i.e., monitoring performance of systems for speed, sending appropriate error messages/alerts when needed, etc).
- To respond to and resolve errors and/or alerts.
- To develop, monitor, and report key performance indicators.
- To establish and track service level agreements.

Project Facilitation & Implementation

- To plan and implement projects to address identified needs as per the ICT strategy.
- To compile project reports on completion of the project to evaluate return on investment.

Budget Optimisation

- To make inputs to the expenditure in line with core activities and projects
- To provide reconciled payments and recover and any overpayments from the systems.

Compliance Monitoring & Evaluation

- To facilitate the process of verification, compliance, registration and deregistration from business.
- To implement identified key controls and established risk mitigation procedures for all the systems.
- To assess and improve of the audit, risk and compliance outlook.
- To implement the audit plan as per ICT strategy.

Information & Knowledge Management

- To collaborate with stakeholders to build systems that enable the management of data obtained from different sources.
- To collaborate with stakeholders to use their experience, education and understanding to obtain knowledge from this information.

Reporting & Accountability

- To report on and account for the unit's cloud system status, the cloud system operational plan progress, cloud systems issues and interventions management, internal and external audit and risk, and any other work in the mandate of the ongoing cloud infrastructure and networks team

NSFAS
National Student Financial Aid Scheme

DESIRED SKILLS AND EXPERIENCE

Minimum requirements:

- Bachelor's degree in information systems or related (NQF 7)
- ITIL
- At least one entry-level information Security certification i.e. RESILIA/ ISO27001/ CISSP, CEH, etc
- Cloud Certification (i.e. AWS, AZURE, Google)
- 5 Experience in LAN, WLAN and WAN networking technologies, etc. CCNA/CCNP/CCDP certified or similar (preferred -Cisco and HP)
- Experience in LAN, WAN, DMZ security, firewalls, WAF, IPS, etc. CEH/FCNSA/CCNA: security certified or similar (preferred -Cisco ASA and FortiGate)
- Experience with web application security and firewalls (preferred -Barracuda)
- Experience with MS Windows, Server, SQL, Exchange, Active Directory, etc.
- Experience with VMWare
- Experience with Linux -Kali, Ubuntu, Debian, Centos, Redhat, Fedora, etc.
- Experience with SAN and Backup technologies, etc.
- Experience with programming and scripting languages, HTML, Java, Python, etc.
- Experience with penetration testing tools and vulnerability scanners, Nessus, Arachni, FOCA, etc.
- Experience with SIEM solutions, Alien Vault, etc.
- Experience with Infrastructure and application monitoring and management tools and software

Preferred:

- Knowledge and Experience of security frameworks and regulations, i.e., NIST, POPIA, ISO 27001.
- Advanced knowledge of the higher education sector

Skill and Competencies:

- Communication skills
- Interpersonal skills
- Data Analysis and Troubleshooting skills
- Presentation skills
- Report writing skills.
- Problem Solving skills.
- Planning skills

REMUNERATION & BENEFITS

Remuneration Package: R 864 336 to R1 018 155 per annum

Total Cost to Company per annum inclusive of all benefits and company contributions

PLEASE NOTE

Closing date: 8 September 2023

Interested applicants must complete and submit an Employment Application Form available on the NSFAS website. The form must be supported by a detailed Curriculum Vitae which includes amongst other things the vacancy name/position title you are responding to, copies of academic qualifications, Identity Document, and names of three contactable referees. The response must be addressed to the attention of Ms. Thokozile Mnikina via the following email address: jobs@nsfas.org.za.

Please note the following contact details are for enquiries about JOB CONTENT ONLY and NOT for application purposes.

For Enquiries please contact: Email: thokozilem@nsfas.org.za

The NSFAS does not consider late applications. The NSFAS talent acquisition team only corresponds with Shortlisted Candidates. Should you not hear from the NSFAS talent acquisition team within 2 months from the closing date, please consider your application unsuccessful.

** NSFAS committed to employment equity. Preference will be given to candidates who improve employment equity considerations **

“NSFAS is committed to providing equal opportunities and practicing affirmative action employment. It is our intention to promote representivity (race, gender, disability) in the organisation through filling of this position and candidates whose appointment will promote representivity will receive preference.