EFC ZAMBIA: CYBER SECURITY ANALYST

1. Position Title: Cyber Security Analyst
2. Date: 1st June 2025
3. Department: Information Technology
4. Job Grade: EFC 5
5. Reporting Officer: IT Manager – Infrastructure and Cyber Security

6. Job Summary

The primary objective of the Cyber Security Analyst is to support a broad range of technologies and liaises across multiple areas of the business to support incidents, problems, requests and changes. They also ensure that EFC's technology and systems are both secure and protected.

The role is responsible for monitoring networks and systems, detecting security threats ('events'), analysing and assessing alarms, and reporting on threats, intrusion attempts and false alarms, either resolving or escalating them, depending on the severity.

7. Duties and Responsibilities

- Research/evaluate emerging cyber-Security threats and vulnerabilities and ways to manage them
- Plan for disaster recovery and create contingency plans in the event of any security breaches.
- Monitor for attacks, intrusions and unusual, unauthorised or illegal activity.
- Test and evaluate security products and check suppliers' certification, compliance and accreditation.
- Design new security systems or upgrade existing ones.
- Use advanced analytic tools to determine emerging threat patterns and vulnerabilities.
- Engage in 'ethical hacking', for example, simulating security breaches.
- Identify potential weaknesses and implement measures, such as firewalls and encryption.
- Investigate security alerts and provide incident response using incident handling methodologies and best practices.
- monitor and respond to common cyber threats such as 'phishing' emails, 'pharming' activity, malware and ransomware.
- Monitor identity and access management, including monitoring for abuse of permissions by authorised system users.
- Liaise with stakeholders in relation to cyber security issues and provide future recommendations.
- Record all findings, actions taken and lessons learned following an incident to strengthen future responses.
- Generate incident reports for both technical and non-technical staff and stakeholders.

- Review and improve security processes.
- Maintain an information security risk register and assist with internal and external audits relating to information security.
- Promote a culture of security amongst colleagues and other stakeholders and support wider security initiatives.
- Assist with the creation, maintenance and delivery of cyber security awareness training for colleagues.
- Provide advice and guidance to colleagues on issues such as spam and unwanted or malicious emails.
- Responsibilities and tasks outlined in this document are not exhaustive and may change, from time to time, as determined by the needs of the company.

Other tasks and responsibilities that will enable the fulfillment of the above noted responsibilities include:

- Build and install PCs, telephony systems, networks and peripheral devices (such as printers, scanners, mobile / smart phones) related to desktop infrastructure, in accordance with EFC standards.
- Provides advice and guidance to colleagues regarding incidents
- Maintain installed PCS, networks, telephone systems and peripherals with routine maintenance.
- Identify, log and resolve technical problems with software applications or network systems.
- Identify potential changes and system improvements to present to senior team leaders for consideration, approval and implementation.
- Ensure that work is carried out within agreed service levels and in accordance with EFC departmental guidelines.
- Create, maintain and distribute reports of progress to senior IT leadership.
- Migrating servers from Windows server 2012 R2 to Windows 2016 or higher platform.
- Maintain client databases with up-to-date solutions and clear record of activities.
- Explain and document technical issues in a clear way to clients.

8. Qualifications & Requirements

- Bachelor's degree in Computer Science, Information Systems, Computer Engineering, Electrical Engineering, Mathematics, Physics or equivalent education from any recognised university.
- Experience working in cyber security in a highly fast paced organisation.
- Expert-level IT skills, including knowledge of networks, data centers, hardware, software and service delivery.

- Certifications in Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) or CompTIA Security+.
- Experience with Vulnerability scanning solutions.
- Understanding of mobile technology and OS (Android, IOS, Windows), VM Ware technology and Linux.

9. Core Competencies:

Technical Skills

- System Administration
- Network protocols, security and troubleshooting (Routers, hubs and switches)
- Information Security policies
- Excellent problem-solving and critical-thinking skills
- Firewall and anti-virus software Administration
- Vulnerability assessment and Penetration Testing including Intrusion Detection
- Good understanding of hacker strategies to anticipate the moves cyber criminals might make.

Other Skills

- Excellent verbal and written communication skills
- Research capabilities
- Planning
- Positive attitude
- Attention to detail