Gambling Control Commission of Trinidad and Tobago ®

CAREER OPPORTUNITY

Cybersecurity Specialist

The Cybersecurity Specialist is a professional responsible for protecting the organization's information systems, ensuring data security, conducting security assessments and responding to security incidents. This role requires a deep understanding of current threats, security controls, best practices for planning and executing security responses. They should also be proficient in risk assessment, incident responses and security architecture. Adept at implementing security protocols and performing threat analysis to safeguard organizational assets.

In addition to specific responsibilities outlined below, the Cybersecurity Specialist should possess strong leadership, communication, problem-solving, and organizational skills.

Key Responsibilities

- Design and implement security measures such as firewalls, encryption and intrusion detection systems.
- Ensure security controls are integrated into the organization’s IT infrastructure.
- Develop and enforce cybersecurity policies and procedures. Educate staff on cybersecurity best practices and policies through training programs
- Identify potential risks and develop strategies to mitigate them. This includes creating risk management plans, logs, monitoring risks, work with management and IT Staff to understand the business impact of various risks and prioritize them accordingly.
- Constantly monitor networks for security breaches and investigate violations.
- Analyse the security measures currently in place and identify potential vulnerabilities.
- Respond promptly to security incidents and provide thorough post-event analyses. Develop and implement incident response protocols to handle breaches effectively.
- Stay updated on the latest cybersecurity threats and trends. Analyse threat intelligence to anticipate and mitigate potential attacks.
- Conduct regular security audits and assessments to ensure compliance with security policies and standards. Identify and rectify security weaknesses through vulnerability assessments and penetration testing.
- Ensure that the organization complies with relevant laws, regulations, and standards (e.g., GDPR, HIPAA, ISO 27001). Prepare for and participate in compliance audits.
- Provide technical support and guidance to other departments on cybersecurity-related issues.
- Troubleshoot and resolve security-related issues as they arise.
- Facilitate effective communication between team members, stakeholders and other relevant parties. Keep stakeholders informed about cyber security risks, current and emerging through regular updates, meetings and reports.

- Maintain detailed documentation of security measures, incidents, and responses.
- Report on security status and incidents to management and stakeholders.

Qualifications and Experience

- A recognized Bachelor's Degree in Computer Science, Computer Information Systems, Information Systems Management, Computer Engineering or a related area.
- Certifications - Certified Information Systems Security Professional (CISSP), CompTIA Security+, a Certified Information Systems Auditor (CISA), Certified Ethical Hacker (CEH) and or equivalent experience as a Cybersecurity Specialist.
- Minimum of three (3) years' experience in a Cybersecurity Specialist role in an Information Technology environment.

Interested Applicants can submit their resumes to: vacancies@gcctt.org