Position Description

JOB TITLE:	**Cyber Security Analyst**
DEPARTMENT:	**Technology Services Group**
REPORTS TO (TITLE):	**Information and Communication Technology Manager**
LAST DATE REVIEWED:	**February 2021**

JOB SUMMARY

The Children's Cancer Institute is embarking on an ambitious 5-year strategic plan with technology underpinning many of the strategic initiatives. As the Institute grows and the pace of innovation in both our Research and Operations continues to grow, we have recognised the need for a dedicated Cyber Security Analyst to help manage and maintain all security across the institutes internal programs, systems, and processes in addition to the products and solutions that are provided to our staff. The increase in these areas has been driven by our Zero Childhood Cancer program and the implementation of a new Computational Biology program at the Institute in 2018 which further increased the need to monitor and secure our network and services from all threats and vulnerabilities in our environment.

The role of the Cyber Security Analyst is to ensure the secure operation and monitoring of the in-house computer systems, servers, and network connections. This includes day-to-day operations of the in-place Security solutions, identification, investigation and resolution of Security incidents and breaches detected by those systems, checking server and firewall logs and scrutinising network traffic. The CSA will also analyse and resolve Security tickets and vulnerability issues in a timely and accurate fashion and conduct user activity audits where required.

PRIMARY TASKS / RESPONSIBILITIES

- Act as the Subject Matter Expert (SME) on cybersecurity and to ensure relevant stakeholders are provided with relevant, accurate and current information on cybersecurity.
- Undertake Cyber Security threat and vulnerability identification and assessments to identify potential cybersecurity weaknesses and recommend appropriate responses to ensure the institutes assets are protected.
- Work with the ICT Manager and CIO to develop, implement, and maintain an Operational Technology Cybersecurity assurance program to ensure the Institute assets are protected.
- Support the management of the Information Security Management System and Cyber Security Management Systems to ensure they meet international standards and the Institute's Cyber Security Policy 2019.
- Provide security assurance leadership to all Departments, as well as vendors, to ensure compliance with applicable cybersecurity policies, standards, legislative and regulatory obligations.
- Manage and control self-assessments and vendor security assessments to ensure effective cybersecurity risk management is in place.
- Provide regular and ad hoc analysis and reports on departmental team's status of cybersecurity performance, potential threats, and issues to ensure management have relevant data to make informed business and resourcing decisions.
- Working with the ICT Manager and CIO to implement, manage and monitor the rollout of the Institute wide Cyber Security training program and ensure effective reporting is in place.

MINIMUM REQUIREMENTS

Essential:

- 3+ years working in Cyber Security field
- Intermediate skills in SIEM operation as an analyst
- Running queries to follow a chain of events through multiple indexes or other sources.
- Broad hands-on knowledge of firewalls, intrusion detection/prevention systems, anti-virus software, data encryption, and other industry-standard techniques and practices.
- In-depth technical knowledge of network and operating systems.
- Understanding common protocols such as TCP, UDP, IPSec, HTTP, SSL, TLS, and DNS.
- Identify threats and work to create steps to defend against them.
- Perform Vulnerability Scans across all network segments and Web Services.
- Monitor network traffic for suspicious behaviour.
- Analyse current Security requirements and make suggestions for improvements.
- Conduct Security audits and make policy recommendations.
- Proven analytical and problem-solving abilities.
- Intuition and keen instincts to pre-empt attacks.

Desirable:

- CEH, OSCP, OSCE, GIAC, GCIA, GSEC, Security+, CISSP or other Security certifications preferred.

General:

- Exhibits high degree of professionalism and respect for others.
- Superior oral and written communication skills
- Ability to maintain privacy and confidentiality.
- Strong ethical work style
- Team player
- Excellent documentation skills
- Excellent negotiation and conflict management skills
- Strong problem-solving skills
- Willingness to undertake after-hours work when required.

KEY SKILLS

- Demonstrable strong personal interest in cyber security
- Knowing when to ask for assistance.
- A keen interest to learn, both in the analyst field and related work areas
- Willingness to go the extra mile for our staff and ensure their mission objectives are met.
- Good social skills and able to interact professionally with a wide range of people.
- Basic understanding of how to query people effectively for information to support investigations whilst being sensitive to limitations of what is acceptable.
- Willingness to undertake exams and perform other tasks to gain appropriate industry qualifications.
- Willingness to be mentored by senior team members.
- Willingness to mentor junior team members
- Contribute to policies, processes and procedures.
- Able to work with minimal supervision.

- Willingness to learn the network and identify appropriate sources of logs or other information to be integrated into the monitoring platform.
- Proactively look for ways to improve the service, either through configuration, process, or other changes as required.
- Previous IT project management experience, planning system implementations and upgrades as well as scheduling day to day maintenance activities.
- Superior interpersonal skills - ability to work closely with all levels of management and staff in order to facilitate optimal outcomes.
- Strong analytical skills
- Ability to work under pressure and autonomously.
- Ability to investigate technology issues and find appropriate solutions.
- Ability to consistently meet or exceed all deadlines.
- Superior attention to detail
- Ability to handle multiple concurrent tasks.

EXPECTED OUTPUTS

- Risk identification for critical systems
- Improving business continuity plans
- Cyber incident management response plans
- TSG user security and privileged user accesses management plans
- TSG security infrastructure up-lift

Children's Cancer Institute policies applicable

- Code of Conduct/Ethics
- Whistleblowing
- Use of Electronic Resources
- Workplace Health & Safety
- Appropriate Workplace Behaviour
- Privacy
- Any other policies not listed here but are available on the Children's Cancer Institute Intranet Policies pages

SERVICE STANDARDS AND GENERAL EXPECTATIONS

- Respond to phone calls and emails within 48 hours.
- Read internal communications within 48 hours.
- Maintain up to date personal information in the HRIS (ConnX - Self Service) at all times.

OUR VALUES

A is for **Accountability** and **Integrity**

C is for **Camaraderie**, **teamwork** and **Sharing.**

E is for **Excellence** and **Success**

S is for **Satisfaction. The result of living our values every day.**

COMPLIANCE AND CODE OF ETHICS AND CONDUCT

Staff members are responsible for ensuring that they are familiar with and comply with their conditions of employment as stated in their individual contract, all Children's Cancer Institute Policies and Procedures and relevant ethical and regulatory guidelines. Staff must be aware that breaches by individuals will not be tolerated or condoned and may be subject to the Disciplinary Action Policy.

Your knowledge and awareness of Children's Cancer Institute Policies and Procedures (including the Code of Ethics and Conduct) will be monitored from time to time to ensure that our compliance program is effective.

Part of compliance adherence involves the use of standardised forms, checklists, and other aids (as appropriate) to ensure that important compliance issues are not overlooked. All forms must be used in accordance with instructions and the procedures as outlined in the relevant policies and procedures to ensure that compliance to the laws and regulations occurs.

WORK HEALTH & SAFETY

- Must adhere to all WHS policies and procedures including reporting incidents within 24 hours.
- Take reasonable care for their own health and safety and the health and safety of other people who may be affected by their conduct in the workplace.
- Actively participating in health and safety meeting, training, and induction programs
- Complying with all safe work procedures and instructions
- Use equipment in compliance with relevant procedures, without wilful interference or misuse.
- Ensure that any hazardous conditions, near misses and injuries are reported immediately to the supervisor and in the WHS reporting system (Myosh)
- Must not wilfully or recklessly interfere with or misuse anything provided in the interest of environment health and safety or welfare.

REPORTING STRUCTURE

Position reports direct to ICT Manager.

Departmental Structure: See Organisation Chart

Note: *Reporting structure may change subject to management decisions and business requirements.*