Cancer Trials Australia
Position Description

Position Details

Position Title:	**Junior Cybersecurity Analyst**
Manager:	Information Systems Manager
Location:	Victorian Comprehensive Cancer Centre (VCCC) Building, 305 Grattan Street, Parkville and working from home office
Key internal working relationships:	• Management Team • Key Application Specialists/Administrators
Key external working relationships:	• Uptake Digital

Position Purpose

This role's primary objective is to ensure our organisation develops a robust cybersecurity framework to protect sensitive information and data, prevent unauthorised access to our systems and enhance employee knowledge of evolving threats and vulnerabilities. This will involve reviewing and building on an existing gap analysis, to document and develop internal work practice guidelines and policies and procedures that will form the governance of CTA's cybersecurity framework, connecting people, process and technology.

This role is responsible for developing CTA's cybersecurity awareness and support culture building by developing learning material for all employees, whilst monitoring and supporting continuous improvement for ongoing growth.

Key Responsibilities

1. Governance, Risk and Compliance

- Prepare for external audit against CTA's selected audit framework utilising existing analyses and internal documentation, establishing measures and controls that meet the selected framework in addition to other relevant industry guidelines.
- Document and develop cybersecurity policies and procedures for asset and inventory management, data lifecycle, data protection, recovery plans, log management, account management and incident management response, supporting CTA's cybersecurity maturity.
- Develop a process to evaluate third party/service providers who hold sensitive data on behalf of CTA to ensure security protections are appropriately managed.
- Identify cybersecurity risks within existing practices and policies and develop appropriate mitigation strategies to reduce internal weakness, vulnerabilities and threats.

2. Analysis and Continuous Improvement

- Monitor the implementation of security policies and guidelines, providing recommendations for ongoing improvement.
- Remain up to date on cybersecurity trends and emerging threats to ensure practices, policies and procedures are relevant and effective.

3. Education and Training

- Assist in the development and delivery of learning materials and training programs and activities to educate all staff on new policies, procedures and security practices.
- Ensure staff understand their cybersecurity responsibilities and are able to recognise and respond appropriately to cybersecurity threats and reporting procedures.

Knowledge, skills and experience

Qualifications:

The minimum educational, technical, or professional qualifications required to competently perform this role include:

- Tertiary level qualification in Cybersecurity, Information Technology, or a related field (or equivalent experience)

Desirable Experience:

- Knowledge of Cybersecurity frameworks (e.g. CIS Critical Security Controls, NIST, ISO 27001) and standards.
- Understanding of network security, threat assessment, and risk management concepts.
- Previous experience or internship in cybersecurity or IT security roles.

Skills and Knowledge:

- Ability to clearly and concisely document and develop Cybersecurity policies and procedures.
- Establish and maintain positive, collaborative relationships with internal and external stakeholders.
- Ability to work autonomously and direct own initiative to achieve agreed objectives.
- High level of organisation and time management skills.
- High level of attention to detail and accuracy.
- Ability to communicate professionally, orally and written.
- Strong sense of professionalism and integrity when dealing with confidential and sensitive information.
- Strong analytical and problem-solving skills.

Our Values

To actively support and demonstrate our organisation values in all work activities and interactions.

Shared Purpose

Integrity

Collaboration

Adaptability

Compassion

Acknowledgement

Employee Name: Date:

Employee Signature:

Manager Name: Date:

Manager Signature: