**JOB TITLE:** Security Architect

**RESPONSIBLE TO:**  CTO

**ACCOUNTABLE TO:** COO, Executive Team, Board, IT Management

**LINKS TO:** IT Team, Compliance, Risk, External Vendors, Safeguarding, Training

**JOB PURPOSE:**

The Security Architect is responsible for designing and implementing robust security frameworks and solutions to protect the organisation's IT infrastructure, applications, and data. This role involves assessing current security practices, identifying vulnerabilities, and developing strategies to mitigate risks while ensuring compliance with relevant regulations and industry standards. The Security Architect will collaborate with cross-functional teams to integrate security best practices into all aspects of the technology environment and will act as a subject matter expert on security-related matters. By fostering a culture of security awareness and proactive risk management, the Security Architect will help safeguard the organisation’s assets and maintain stakeholder trust.

**KEY ACCOUNTABILITIES:**

* Design and implement a comprehensive security architecture framework that aligns with the organisation's strategic objectives and compliance requirements.
* Conduct regular security assessments to identify vulnerabilities, threats, and risks, and develop mitigation strategies to address them.
* Develop and enforce security policies, standards, and guidelines to ensure that all IT systems and processes adhere to best practices and regulatory requirements.
* Establish and maintain an incident response plan, ensuring effective procedures are in place to respond to security breaches and minimize impact.
* Work closely with IT, operations, and business units to integrate security measures into all technology projects and initiatives.
* Promote security awareness across the organisation by providing training and resources to staff, fostering a culture of security mindfulness.
* Evaluate and manage relationships with third-party vendors, ensuring their security practices meet organisational standards and do not pose risks.
* Review and assess existing security solutions, making recommendations for enhancements or replacements to improve overall security posture.
* Ensure compliance with relevant laws, regulations, and industry standards related to information security, data protection, and privacy.
* Drive continuous improvement in security practices and technologies, staying informed about emerging threats and industry trends to adapt the security architecture accordingly.

**EXPERIENCE & QUALIFICATIONS:**

**Essential Experience and Qualifications:**

1. **Education:**
   * Bachelor’s degree in Computer Science, Information Technology, Cybersecurity, or a related field.
2. **Experience:**
   * A minimum of 5 years of experience in information security, with a focus on security architecture and design.
   * Proven track record of developing and implementing security frameworks and policies in complex environments.
   * Experience conducting security assessments, risk analysis, and vulnerability management.
3. **Technical Skills:**
   * Strong understanding of security technologies, including firewalls, intrusion detection/prevention systems, encryption, and identity management.
   * Familiarity with compliance frameworks such as ISO 27001, NIST, GDPR, and relevant industry regulations.
4. **Certifications:**
   * Relevant security certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or Certified Ethical Hacker (CEH).
5. **Analytical Skills:**
   * Excellent analytical and problem-solving skills, with the ability to assess security risks and develop effective mitigation strategies.
6. **Soft Skills:**
   * Strong communication and interpersonal skills, with the ability to effectively engage and influence stakeholders at all levels.
   * Ability to work collaboratively in a team-oriented environment while also being self-motivated.

**Preferred Experience and Qualifications:**

1. **Education:**
   * Master’s degree in a relevant field (e.g., Cybersecurity, Information Assurance).
2. **Certifications:**
   * Additional certifications such as Certified Cloud Security Professional (CCSP), Certified Information Systems Auditor (CISA), or TOGAF (The Open Group Architecture Framework).
3. **Experience:**
   * Experience in the education sector or with organisations focused on social care or special education.
   * Previous experience with cloud security architecture and managing security in cloud environments.
4. **Technical Skills:**
   * Knowledge of security tools and technologies for monitoring, detection, and response (e.g., SIEM solutions, endpoint protection).
   * Familiarity with secure software development practices and DevSecOps principles.

**QUALITIES AND BEHAVIOURS:**

* Hold and articulate clear values
* Demonstrate optimistic personal behaviours, positive relationships and attitudes towards colleagues, and wider internal and external contacts
* Lead by example, demonstrating integrity, creativity, resilience and clarity
* Highly motivated and resilient

**ADDITIONAL REQUIREMENTS:**

* Act as an ambassador for Outcomes First Group
* At all times promote and comply with organisations commitment to safeguarding, equal opportunities and health and safety

Please note the role specification is subject to change as part of the dynamic nature of the business.

**Job Holder’ signature**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed on behalf of Outcomes First Group**

Name: : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_