|  |  |  |
| --- | --- | --- |
| **SAVE THE CHILDREN INTERNATIONAL ROLE PROFILE** | |  |
| Position Title: | SCA Information Security Specialist |

|  |  |  |  |
| --- | --- | --- | --- |
| **Team** | Cybersecurity and Information Assurance, TDIT | **Grade** | P3 |
| **Reports To** | Head of SCA Information Security Services | **Contract Length** | Permanent |
| **Location [Physically based in]** | Remote | **Time-zone [the time-zone that the role holder must be available to work in]** | Global |
| **Language(s)** | English *[Fluency in English as a minimum is required for all roles due to working in a Global team]* | **Positions available** | 4 |

|  |
| --- |
| **Team and Job Purpose** |
| **Team purpose**  The Information Security Specialist role is critical to increasing and then maintaining security maturity across Save The Children Association (SCA) Members, allowing them to meet their obligations under the Mutual Accountability Framework minimum standard for information security.  **Role purpose**  The Information Security Specialist will act as the primary contact for information security matters between SCA Member organisations and SCI within the region to which they are assigned and offer independent objective advice, guidance and support for the senior leadership teams and functional teams.  They will also be required to lead or assist with incident management processes both in SCI and SCA Members.  Ultimately, the Information Security Specialist will help achieve and maintain SCA and SCI compliance through the implementation of transparent IT Security policies, systems and procedures. |

|  |
| --- |
| **Principal Accountabilities** |
| **Information Security Assessment**   * Carrying out regular assessments of current information security practices across SCA Member organizations. * Supporting the delivery of vulnerability assessments and penetration tests (and other Shared Services) with the SCI Information Security & Assurance team. * Establish key performance indicators (KPIs) to measure the effectiveness of security initiatives. * Regularly report on security metrics and progress toward maturity goals to the Head of SCA Information Security Services.   **Policy Development and Implementation**   * Support and advise the Member’s Point of Contacts (PoC) during the implementation, and maintenance of IT security policies, standards, and procedures. This could include the writing and reviewing of new policies and procedures. * Ensure Member policies align with the Mutual Accountability Framework and other regulatory requirements and are implemented effectively within the Member.   **Training and Awareness**   * Support the delivery of Member information security training programs for staff at all levels, including training content and phishing simulations. * Foster a culture of security awareness within the organization.   **Incident Management Support**   * Assist in information security incident management processes, including identification, containment, eradication, recovery and testing. * Coordinate communication and reporting of security incidents to relevant stakeholders.   **Stakeholder Engagement**   * Serve as the primary point of contact for information security matters within assigned regions. * Develop strong working relationships with Member PoCs and other key stakeholders. Provide expert advice and support to senior leadership and functional teams on all issues relating to information security. * Prepare and present reports on security compliance and maturity to senior management.   **Risk Management**   * Support risk assessment activities to identify and prioritize potential security threats. Support the development of appropriate risk management processes where not in place. * Recommend risk mitigation strategies and monitor their effectiveness.   **Collaboration and Communication**   * Collaborate with IT teams and other departments to integrate information security into all business processes. * Help facilitate clear and regular communications regarding security initiatives and concerns.   **Continuous Improvement**   * Stay informed about the latest trends and best practices in information security. * Recommend improvements to security strategies based on industry developments and organizational needs. |

|  |
| --- |
| **Budget** |
|  |

|  |
| --- |
| **People Management Responsibility** (direct/indirect reports) |
| Number of people managed in total: None  Manager of a team: No  Team Manager (manager of multiple teams): No |

|  |
| --- |
| **Size of Remit** |
| Global |

|  |
| --- |
| **Travel Requirements** |
| International travel required: Yes  Percentage of required for travel: 5-10% |

|  |
| --- |
| **Key Relationships** |
| **Internal** (excluding direct team and manager)   * SCI Information Security and Assurance team * SCI IT team   **External**   * SCA Members * Third-party vendors |

|  |
| --- |
| **Competencies** |
| Competency: Leading and Inspiring Others  Level: Accomplished  Behavioural Indicator: Takes a flexible and positive leadership style adapting to a given situation or to the needs of the team  Competency: Applying technical and professional expertise  Level: Accomplished  Behavioural Indicator: Applies the required technical and professional expertise to the highest standards; promotes and shares best practice within and outside the organisation.  Competency: Communicating with impact  Level: Accomplished  Behavioural Indicator: Communicates clearly and confidently with others to engage and influence; promotes dialogue and ensures timely and appropriate messages, building confidence and trust.  Competency: Delivering results  Level: Accomplished  Behavioural Indicator: Takes personal responsibility and holds others accountable for delivering our ambitious goals for children, continually improving their own performance or that of the team/ organisation.  Competency: Problem solving and decision making  Level: Accomplished  Behavioural Indicator: Invests time and energy to actively develop self and others to help realise their full potential, and to build the organisation’s capability for the future.  Competency: Working effectively with others  Level: Accomplished  Behavioural Indicator: Works collaboratively to achieve shared goals and thrives on diversity of people and perspectives; knows when to lead and when to follow and how to ensure effective cross-boundary working. |

|  |
| --- |
| **Experience and Skills** |
| **Essential**   1. Good knowledge of ISO/IEC 27001 and NIST Cybersecurity Framework (CSF) 2. At least two years of experience working in an information security programme or project environment 3. Good understanding of IT infrastructure including cloud, networks and information management systems 4. Capability to convey technical information effectively to non-technical stakeholders in a clear and comprehensive manner 5. Ability to work with a range of business stakeholders to understand and articulate their activities in line with defined standards 6. Good verbal and written communication skills (in English) 7. Self-motivated, with a proactive and collaborative approach, and a strong results orientation 8. Commitment to Save the Children mission and values |

|  |
| --- |
| **Education and Qualifications** |
| **Essential**  • Degree or diploma in Computer Science / Business Technology / Information Security, or relevant experience  **Desirable**  • Security related certification/s |

|  |
| --- |
| **Safeguarding** |
| We need to keep children and adults safe so our selection process includes rigorous background checks and reflects our commitment to the protection of children and adults from abuse.  Level 1:  A basic criminal record background (DBS) check is required/equivalent police record check. |

|  |
| --- |
| **Diversity, Equity and Inclusion and Equal Opportunities** |
| Diversity, Equity and Inclusion is core to our vision, values and global strategy. Save the Children is committed to creating a truly diverse, equitable and inclusive organisation, and one which will support us in our vision to ensure every child attains the right to survival, protection, development, and participation.    We are committed to equal employment opportunities, regardless of gender, sexual orientation, race, colour, ethnic origin, nationality, disability, marital or civil partnership status, gender reassignment, pregnancy and maternity, caring or parental responsibilities, age, or beliefs and religion. We are committed to diversifying our staff to better represent the communities we serve and actively welcome underrepresented groups to apply.    Reasonable adjustments will be made should any candidate invited to interview require this. |

|  |
| --- |
| **Additional job responsibilities** |
| The duties and responsibilities as set out above are not exhaustive and the role holder may be required to carry out additional duties within reasonableness of their level of skills and experience. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Control and Approval** | | | | |
| Version | Date | Author | Reviewer | Approver |
| 0.1 | 26/11/2024 | Audrey Zambrano |  | Gareth Packham |