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

|  |  |  |  |
| --- | --- | --- | --- |
| **Team** | Cybersecurity and Information Assurance, TDIT | **Grade** | P3 |
| **Reports To (Title)** | Head of Information Security Services | **Contract Length** | Permanent |
| **Location [Physically based in]** | Any existing SCI office location | **Time-zone [the time-zone that the role holder must be available to work in]** | N/A; Global |
| **Language(s)** | English | **Positions available** | 4 |

|  |
| --- |
| **Team and Job Purpose** |
| **Team purpose**  The SCA Information Security and Data Protection Team is responsible for supporting our Members in safeguarding the confidentiality, integrity, availability of all information assets (data and systems). The team is responsible for identifying, assessing and managing Member information security and data protection risks and helping Members improve their information security programmes.  **Role purpose**  The SCA 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.  This role will also work closely with the SCI Information Security and Data Protection Team to promote the sharing of best practice and ensure alignment between SCI and Member information security and data protection programmes. |

|  |
| --- |
| **Principal Accountabilities** |
| * Carrying out regular assessments of current information security practices across SCA Member organizations (with appropriate reporting of status to key stakeholders). Help Members establish key performance indicators (KPIs) to measure the effectiveness of their information security programme. * Supporting Members to complete the annual Mutual Accountability Framework self-assessment and coordinating resulting mitigation plans * Support risk assessment activities to identify and prioritize potential security threats. Support the development of appropriate risk management processes where not in place. * Supporting the delivery of vulnerability assessments and penetration tests (and other Shared Services) with the SCI Information Security & Assurance team. * 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. * Support the delivery of Member information security training programs for staff at all levels, including training content and phishing simulations. Foster and grow a culture of security awareness within the organization. * Assist in information security incident management processes, including identification, containment, eradication, and recovery. Coordinate communication and reporting of security incidents to relevant stakeholders. * 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. * Stay informed about the latest trends and best practices in information security; recommend improvements to security strategies based on industry developments and organizational needs. * Collaborate with SCI IT and Information Security Teams to ensure alignment of information security tools and best practices across the movement. Help facilitate clear and regular communications regarding security initiatives and concerns. |

|  |
| --- |
| **Budget** |
| N/A |

|  |
| --- |
| **People Management Responsibility** (direct/indirect reports) |
| Number of people managed in total: 0  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)   * Information Security and Data Protection Team; IT Global Operations Team; Global Safety and Security; Country Offices   **External**   * Member IT / InfoSec leads and Members Senior Management Teams * Cybersecurity vendors and partners * External auditors |

|  |
| --- |
| **Competencies** |
| Cluster: Leading 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.  Cluster: Leading Competency: Delivering results Level: Accomplished Behavioural Indicator: Establishes clear and compelling objectives with teams and individuals and monitors progress and performance.  Cluster: Thinking Competency: Problem solving and decision making Level: Accomplished Behavioural Indicator: Makes informed strategic decisions based on full evaluation of the opportunities and risks of each idea and solution.  Cluster: Thinking Competency: Innovating and adapting Level: Accomplished Behavioural Indicator: Openly talks about doing things differently, pushing boundaries and ways of working to drive improvements.  Cluster: Engaging Competency: Working effectively with others Level: Accomplished Behavioural Indicator: Enables people from a wide range of backgrounds and perspectives to contribute to positive outcomes.  Cluster: Engaging Competency: Communicating with impact Level: Accomplished Behavioural Indicator: Conveys complex issues with clarity, brevity and confidence. |

|  |
| --- |
| **Experience and Skills** |
| **Essential**   1. Experience working on cybersecurity, information security and data protection requirements within a global organization or related, technical or IT support. 2. Good understanding of IT infrastructure including cloud, networks and information systems. 3. Good knowledge of the current information security threat landscape 4. Capability to convey technical information effectively to technical and non-technical stakeholders in a clear and comprehensive manner. 5. Capacity to build and maintain excellent relations and to work effectively in a multicultural and multi-ethnic environment respecting diversity. 6. Strong personal, organisational and self-management skills. 7. Strong communication skills, in English. 8. Commitment to Save the Children mission and values   **Desirable**   * Strong working knowledge of ISO/IEC 27001 and NIST Cybersecurity Framework (CSF) * Experience of ‘field operations’ and the cybersecurity-related issues associated with working in remote, inhospitable and insecure environments * Strong understanding of/willingness to learn key trends in international and humanitarian development and how technology can and is being utilised to support these developments |

|  |
| --- |
| **Education and Qualifications** |
| **Essential**  Degree or diploma in Computer Science / Business Technology / Cybersecurity / Information Security, or relevant experience  **Desirable**  Cybersecurity 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 2: either the post holder will have access to personal data about children and/or young people as part of their work; or the post holder will be working in a ‘regulated’ position (accountant, barrister, solicitor, legal executive); therefore a police check  will be required (at ‘standard’ level in the UK or equivalent in other countries). |

|  |
| --- |
| **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. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Control and Approval** | | | | |
| Version | Date | Author | Reviewer | Approver |
| 0.1 | 15/11/2024 | G Packham |  |  |
| 0.2 | 08/04/2025 | G Packham |  |  |