|  |  |  |
| --- | --- | --- |
| **SAVE THE CHILDREN INTERNATIONAL ROLE PROFILE** | |  |
| Position Title: | SCA Data Protection Specialist |

|  |  |  |  |
| --- | --- | --- | --- |
| **Team** | Cyber Security and Information Assurance | **Grade** | P3 |
| **Reports To** | Head of Information Assurance and DPO | **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 | **Positions available** | 3 |

|  |
| --- |
| **Team and Job Purpose** |
| **Team purpose**  The Data Protection Shared Services is critical to increasing and maintaining the maturity of privacy and data protection management capabilities across Save The Children Association (SCA) Members, allowing them to meet their obligations under the Mutual Accountability Framework minimum standard for information security and SCARF (internal risk framework). The role reports to the Head of Information Assurance who is responsible for SCAs Information Assurance and Data Protection maturity and global compliance.  **Role purpose**  The Data Protection Specialist will act as the primary contact for data protection 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 / data breach processes both in SCI and SCA Members. |

|  |
| --- |
| **Principal Accountabilities** |
| **KEY AREAS OF ACCOUNTABILITY:**  **Data Protection Assessment**   * Carrying out regular assessments of current data protection practices across SCA Member organizations. * Supporting the delivery of Data Protection Impact Assessment (DPIAs), supplier due diligence (and other Shared Services) with the SCI Information Security & Assurance team. * Establish key performance indicators (KPIs) to measure the effectiveness of privacy and data protection initiatives. * Regularly report on privacy and data protection metrics and progress toward maturity goals.   **Policy Development and Implementation**   * Support and advise the Member’s Point of Contacts (PoC) during the implementation, and maintenance of data protection 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, SCARF and other regulatory requirements and are implemented effectively within the Member.   **Training and Awareness**   * Support the delivery of Member information security and data protection training programs for staff at all levels, including training content and phishing simulations. * Foster a culture of information security and data protection awareness within the organization.   **Incident Management Support**   * Assist in information security incident and personal data breach management processes, including identification, containment, eradication, recovery and testing. * Coordinate communication and reporting of incidents to relevant stakeholders.   **Stakeholder Engagement**   * Serve as the primary point of contact for information security and data protection 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 information security and data protection compliance and maturity to senior management.   **Risk and Compliance Management**   * Support risk assessment activities to identify and prioritize potential security and privacy threats. Support the development of appropriate risk management processes where not in place. * Recommend risk mitigation strategies and monitor their effectiveness. * Support Member’s compliance with local data protection and privacy legal requirements   **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** |
| TBC |

|  |
| --- |
| **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** |
| *Multiple countries or Functions* |

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

|  |
| --- |
| **Key Relationships** |
| **Internal**   * TDIT * Global Safety and Security * Legal   **External**   * SCA Members IT and information security/data protection teams * 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: Maintains both a broad strategic perspective and an awareness of the detail of a situation.  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: Applying technical and professional expertise Level: Accomplished Behavioural Indicator: Shares knowledge and best practice on technical solutions so that others can make best use of that expertise.  Cluster: Engaging Competency: Working effectively with others Level: Accomplished Behavioural Indicator: Breaks down silo working and challenges behaviours that are not collaborative.  Cluster: Engaging Competency: Communicating with impact Level: Accomplished Behavioural Indicator: Conveys complex issues with clarity, brevity, and confidence. |

|  |
| --- |
| **Experience and Skills** |
| **Essential**   * Good knowledge of data protection frameworks such as NIST. * Good understanding of IT infrastructure including cloud, networks and information management systems * Experience with OneTrust or other tools * Capability to convey technical information effectively to non-technical stakeholders in a clear and comprehensive manner. * Ability to work with a range of business stakeholders to understand and articulate their activities in line with defined standards * Good verbal and written communication skills (in English) * Self-motivated, with a proactive and collaborative approach, and a strong results orientation * Commitment to Save the Children mission and values.   **Desirable**   * Two years of experience working in data protection program or project environment * Experienced working for INGOs or NGOs * Data Protection related certification/s such as CIPP |

|  |
| --- |
| **Education and Qualifications** |
| **Essential**  Degree or diploma in Information Security, Law, or relevant field  **Desirable**  Data Protection related certification/s such as CIPP |

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

|  |
| --- |
| **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 |
| 1.0 | 30/09/2024 | Pratigya Bhattarai |  | Gareth Packham |