SAVE THE CHILDREN INTERNATIONAL ROLE PROFILE

Save the Children

Position Title:	Director of Information Security, Data Protection and Global IT Operations

Team	Information Security, Data Protection and Global IT Operations	**Grade**	M5
Reports To (Title)	Chief Information Officer	**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]**	Any
Language(s)	English	**Positions available**	1

Team and Job Purpose

Team purpose

The Information Security, Data Protection and Global IT Operations team is at the forefront of ensuring technology is delivered across SCI in a safe, secure and effective manner. The team is responsible for the maintenance and continual improvement of SCI's Information Security and Data Protection management programme including the delivery of key services such as cybersecurity operations, IT risk management and governance and compliance with key data protection and privacy legislation. The team is also responsible for ensuring the delivery of IT across SCI's global country and regional offices, is maintained in line with SCI standards and is fit for purpose.

Role purpose

The primary purpose of this role is to safeguard the confidentiality, integrity and availability of all SCI's information assets through the implementation, maintenance and enhancement of key information security and data protection controls. The role holder will ensure that information security risks across both SCI and Save the Children Association are identified and mitigated through compliance with the SCA Global Cybersecurity standard. The role will advise the SCI SLT, Member CEOs and the SCA Audit & Risk Board Committee on compliance and risk in these areas. Responsibilities will include the design and implementation of information security and data protection strategy and annual roadmaps, reviewing and setting global standards, risk management, data protection and privacy management.

Through the Head of Global IT Operations (a direct report) and team of Regional IT Operations Leads, the role will ensure all SCI Country Offices and Field Offices deliver safe, secure and effective IT operations to support our global humanitarian programmes, driving compliance to SCI standards and ensuring IT delivery is fit for purpose.

Through leadership of the SCA Information Security and Data Protection Service, the role holder will work with Member IT and Information Security Leads to deliver a consistent approach to information security and data protection management across the movement and deliver cost-effective tools and services through the shared service catalogue.

The Director of Information Security, Data Protection and Global IT Operations will also be expected to act as SCI's Data Protection Officer (DPO) pending a review of data protection capabilities and strategy.

The role will lead on major incidents relating to Information Security and Data Protection within SCI and will form a key member of the Crisis Management Team for SCI and Members where required.

Principal Accountabilities

- Lead the development and continual improvement of SCI's information security and data protection programme to ensure adequate protection for SCI against information security and privacy risks whilst balancing the application of controls with enabling SCI business operations.
- Identify, manage and direct remediation of IT and business risks and compliance gaps in order to maintain appropriate and adequate information security and data protection.
- Act as SCI's Data Protection Officer (DPO) and ensure SCI maintains compliance with UK GDPR requirements, providing appropriate policy, process and standards to ensure all data handled in accordance with required practices. This role will chair the SCI Data Security and Privacy Working Group
- Direct the provision and delivery of global SCA Information Security (chairing the SCA Information Security Steering Committee) and Data Protection Service for Members ensuring that appropriate value adding services are delivered that reduces key risk and enhances security maturity across the organisation.
- Lead on crisis management response to major security and data protection incidents, leading engagement with SCI Crisis Management Team and external authorities as needed.
- Promote a culture of cybersecurity excellence by coaching and mentoring IT members and internal stakeholders, leading by example setting standards of integrity and good practice.
- Ensure 'secure by design' is embedded into all technology initiatives through the Architecture Design Board and TDIT Change Request (TDIT CR) process.
- Support SCI's wider risk management efforts (the SCA Risk Framework or 'SCARF' by acting as Senior Risk Owner for Cybersecurity and Data Protection and membership of SCI's Senior Risk Leadership Group (SRLG)
- Ensuring the Global IT Operations team hold COs to account for the delivery of safe, secure and effective IT services and that CO's adhere to SCI standards and policies for IT delivery. Where any risk is identified, hold RDs/CDs to account for the delivery of the remediation plan to agreed timelines.
- Ensure technology suppliers and 3rd party technology services are fit for purpose with information security and are compliant with SCI information security and data protection policies, procedures and standards, and adhere to SCI Technology Minimum Requirements.

Budget

c.$5m

People Management Responsibility (direct/indirect reports)

Number of people managed in total: c. 26
Manager of a team: Yes
Team Manager (manager of multiple teams): Yes

Size of Remit

Global

Travel Requirements

International travel required: Yes

Percentage of required for travel: 5%

Key Relationships

Internal (excluding direct team and manager)

- ELT
- TLT and Member functional Leads for Shared solutions
- Regional Directors
- Senior Stakeholders from across the movement
- Product Owners

External

- Third party vendors and suppliers
- Consultant/interim resource providers

Competencies

Cluster: Leading
Competency: Leading and inspiring others
Level: Leading Edge
Behavioural Indicator: Develops a compelling and inspired vision or sense of core purpose and clearly communicates it to inspire and motivate others.

Cluster: Leading
Competency: Delivering results
Level: Leading Edge
Behavioural Indicator: Drives a performance culture that aligns to strategic goals through a clear focus on outcomes.

Cluster: Thinking
Competency: Strategic thinking
Level: Leading Edge
Behavioural Indicator: Understands and navigates the long-term strategic context, recognising opportunities and threats, and reshaping strategies accordingly.

Cluster: Thinking
Competency: Decision making
Level: Leading Edge
Behavioural Indicator: Makes high-stakes decisions confidently in the absence of complete information, balancing intuition with a rigorous analysis of available data.

Cluster: Engaging
Competency: Building collaborative relationships
Level: Leading Edge
Behavioural Indicator: Establishes critical and strategic professional networks and alliances that enhance success at both organisational and personal levels.

Cluster: Engaging
Competency: Influencing
Level: Leading Edge
Behavioural Indicator: Positively influences decision-making at the highest levels through sophisticated strategies and understanding of human behaviour.

Experience and Skills

Essential

1. Information Security Expertise: Strong understanding of security frameworks such as ISO 27001,

and NIST CSF. Proficient in risk assessment methodologies, security technologies, knowledge of current IT and privacy laws, specifically GDPR, and their implementation in a global context.

2. Significant Experience in Information Security Management: Leadership in designing and implementing security frameworks and governance models capable of providing effective security and risk management whilst balancing cost vs value and risk.
3. Strategic Vision and Leadership: Ability to develop and implement strategic security initiatives, with leadership skills to manage and guide cross-functional teams and capacity to influence stakeholders and drive cultural change towards cybersecurity and data protection excellence.
4. Crisis Management and Incident Response: Skills in effectively managing and responding to major high profile security incidents and able to engage with external authorities during crises. Experienced in developing and testing disaster recovery and business continuity plans.
5. Communication and Collaboration: Excellent communication skills for articulating complex security concepts to diverse audiences. Able to build and sustain effective relationships with internal teams, external partners, and stakeholders.
6. Training and Mentorship: Proficient in developing and delivering information security training programs. Able to coach and mentor team members and stakeholders, fostering a culture of continuous learning and integrity
7. Supplier and Vendor Management: Skills in assessing and ensuring third-party compliance with security standards. Able to manage vendor relationships to ensure service delivery aligns with organisational security policies.
8. Considerable Experience with Risk and Compliance Management: Identifying and mitigating IT and business risks effectively and ensuring organisational policies comply with regulations like GDPR.
9. Experience in Crisis Management: Proven track record of leading crisis management responses to complex security incidents.
10. Substantial Experience in Cultural and Organisational Change: Promoting cybersecurity and data protection awareness across organisations.

Desirable

- Experience of ‘field operations’ and the IT Security-related issues associated with working in remote, inhospitable and insecure environments
- A second language preferably Spanish.

Education and Qualifications

Essential:

- A degree in Computer Science, Information Technology or a related field is preferred.
- Equivalent practical experience may be considered.
- Professional qualification in Cybersecurity (CISM, CISSP or equivalent)
- Familiarity with information security frameworks, tools and technology

Desirable:

- Data Protection or Privacy qualification (e.g. CIPP/E or C-DPO)
- Professional qualifications in service management (ITIL), risk management, project management (e.g., PMP, Scrum Master) will be beneficial.

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: <u>either</u> the post holder will have access to personal data about children and/or young people as part of their work; <u>or</u> 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
0.2	18 July 2025	J McGovern		