Information Security Officer

Duration:	Permanent
Salary:	Circa £58,000 per annum
Level:	Level 3
Hours:	35 hours per week. Other flexible arrangements will be considered.
Disclosure Level:	Basic. This role involves no direct or indirect work with children.
Reports to:	Chief Information Officer
Location:	Working from home and 1 Westfield Avenue, London E20 1HZ

At the UK Committee for UNICEF (UNICEF UK), we pull together to achieve the best possible results for children in danger around the world. We believe in an inclusive workplace and in the power of fulfilled colleagues who share the same values and goals, enjoy their work, and are motivated to do their utmost for children.

Our work is guided by the UN Convention of the Rights of the Child (UNCRC) and the Sustainable Development Goals (SDGs), which recognise the universality of children's rights.

ABOUT THE TEAM

The Technology Team is part of UNICEF UK's Information Directorate, which is responsible for technology, data management and data analytics to support our fundraising and UK and international programme activities. Ours is a modern, SaaS-based IT environment without the burden of hard-to-maintain legacy systems. Key systems in use include M365, SharePoint, Salesforce, Unit4, Snowflake Datacloud and Asana. Our website www.unicef.org.uk represents our work to the outside word and is a key tool in our fundraising and reputation-building activities. As the UK arm of one of the world's most high-profile charities the integrity of the data we rely on and our reputation for ethical stewardship is of the utmost importance.

ABOUT THE ROLE

The Information Security Officer is responsible for overseeing and implementing information security standards on behalf of and in collaboration with the organisation.

The Information Security Officer will explain technical and contractual issues to colleagues and suppliers and present technical information to non-specialist audiences. This role will direct and motivate colleagues in all areas of the organisation, providing clear and authoritative instructions and advice on security issues, defining acceptable operating practices, and intervening quickly where required.

What we will expect you to achieve

- To maintain oversight of the UNICEF UK's information security, including monitoring the work of our outsourced ICT support team and 3rd party security service providers. To ensure their work continues to protect UNICEF data and continually enhances our security posture.

- To maintain UNICEF UK's compliance with target security standards (including CIS and Cyber Essential Plus) and to achieve compliance with additional standards as defined by our security policies.

- To assess and manage risks associated with third-party suppliers by conducting thorough security evaluations and audits. Develop and enforce policies to ensure suppliers comply with the UNICEF UK's security standards and requirements.

- To continue to strengthen the information security culture of the organisation and design, develop, and deliver security training programmes to increase colleague awareness and understanding of information security practices.

- To keep up to date with developments in security technologies and threats: to ensure your continuous learning is translated into ongoing improvements in UNICEF UK's security.

- To demonstrate a deep understanding of our security toolset and how it should be applied. To ensure that our investment in security is proportionate and effective.

- To document security standards and procedures. To evidence security controls when required including for audits, incident reports and investigations.

- To prepare operational and strategic management information on UNICEF UK's information security performance.

- To carry out day-to-day management of security procedures, and develop, implement, maintain and test a comprehensive incident response plan to address potential security breaches and incidents. Manage security incidents to completion including reporting, follow-up and review.

- To collaborate closely with Legal and Data Protection teams to ensure alignment with regulatory requirements and to address any legal implications of security policies and practices. Provide expert advice on information security matters to support compliance initiatives.

- To demonstrate and model a commitment to our shared values, behaviours and inclusive practices (known as Our Shared Commitment) in all aspects of your work.

BEHAVIOURS, EXPERIENCE AND SKILLS

Effective behaviours

Supporter driven and mission aligned.

- Is committed to children and their rights and motivated to work towards creating a better world for every child.

Communication

- Able to communicate convincingly with stakeholders, presenting technical information clearly and distinguishing what is relevant for each target audience. Communication must be accurate, succinct, timely and appropriate for the purpose and audience.

Results Focused

- Never loses sight of the priority of UUK's business outcomes, taking a pragmatic view of the balance between security, productivity, and compliance.

Principles

- Understands the importance of this role in maintaining UUK's reputation. Acts at all times with the highest levels of probity and honesty in their communications with staff, management, suppliers, auditors and the public.

Analytical

- Makes calm judgements based on researched facts and does not take every piece of information at face value without considering the context.

Relevant experience

- Management of ICT security services and cyber security incidents in a comparable setting
- A solid understanding of IT networking, applications and endpoint security
- Deep and broad knowledge and some working experience in network management, IT security, server or applications administration
- Experienced in developing and writing security policies and applying security principles
- Experienced in managing and maintaining security in a SaaS / hybrid environment
- Comfortable in knowing how to creating technical and end-user documentation for technical and non technical users.
- Good experience in designing and delivering user education sessions and interventions

Specific knowledge and skills

Skills

- Achievement in a previous role of accredited organisational security standards (e.g. Cyber Essentials +, ISO27001, NIST, CIS)
- Highly developed personal organisational skills
- Well-developed people skills (i.e. communication, relationship development and management, patience, conflict resolution and teamwork)
- Good ability to assimilate and communicate information

Knowledge

Good working knowledge of Microsoft 365 and Microsoft Defender along with several of the following:

- **Technologies**: Microsoft 365, Microsoft Defender, Microsoft Windows and Azure
- **Cloud Security:** In-depth understanding of cloud security principles and practices for platforms such as AWS, Google Cloud, and Azure.
- **Network Communications and Architecture:** server, endpoint and email configuration and security issues.
- **Security Frameworks and Standards:** Familiarity with security frameworks and standards such as NIST, ISO 27001, and COBIT.
- **Penetration Testing and Vulnerability Assessment:** Experience with penetration testing and vulnerability assessment tools and methodologies.
- **Data Privacy Regulations:** Knowledge of data privacy regulations including GDPR and PECR.
- **Security Automation and Orchestration:** Proficiency in using security automation and orchestration tools to enhance security operations.
- **Advanced Threat Detection:** Expertise in advanced threat detection techniques, including the use of machine learning and artificial intelligence.
- **IT Service Management**: a working knowledge of ITIL and IT service management issues and concepts, including change management.
- **Professional Certification:** Qualified with AZ 500 or higher Microsoft qualifications, CISSP, CISM or CCSP, Security Administrator Associate or equivalent.
- **Cyber Security Trends:** contemporary insights into threats, tools and responses using a range of sources of current information and support on cyber security.
- SFIA Level 5