ICT Security Manager

Duration:	Permanent
Salary:	£58,000 per annum
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:	Head of Technology
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.

ABOUT THE ROLE

UNICEF UK needs an ICT Security Manager who can take responsibility for overseeing and implementing ICT security standards in this organisation of 400 hybrid-working UK colleagues.

You will need to have a solid understanding of IT networking and endpoint security derived from several years' experience in roles which may have included IT support, network management, server, or core applications administration. Your role at UNICEF will draw on your specialist technical knowledge, your highly developed personal organisational skills and your ability to assimilate and communicate information. This is a key role in a small in-house team, working alongside an outsourced service provider which is thoroughly and successfully integrated with UNICEF's ICT service. You will have regular contact with other colleagues responsible for data governance and DPA compliance and for training.

Working at UNICEF UK you will not be bogged down by bureaucracy or indecision. You will find colleagues who are responsive and committed to success, in an organisation where collaboration and opportunities for learning are welcomed. We are looking for a team member who seeks responsibility, works collaboratively, and can develop the scope of this new role. UNICEF UK will support your learning and career development, which we consider essential to your ability to perform the role.

Without formal line-management responsibility you will need to be able to 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 you see significant security risk.

You will need a good understanding of Microsoft E365 including Microsoft Defender as well as ITIL standards, change control processes and risk investigation and assessment. You must be comfortable discussing technical and contractual issues with colleagues and suppliers and be confident presenting technical

information to non-specialist audiences. You will have excellent written communication evidenced by the quality of documentation and reports you have written.

What we will expect you to achieve

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

- Maintain UNICEF UK's compliance with target security standards and to achieve compliance with additional standards as defined by our security policy.

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

- 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.

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

- Carry out day-to-day management of security procedures, ensuring that security incidents or threats are identified and resolved promptly.

- Manage security incidents to completion including reporting, follow-up and review.

- 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.
- Understands the importance of this role in maintaining UNICEF UK's reputation

Communication

- Communicates convincingly with stakeholders, presenting technical information clearly and distinguishing what is relevant for each target audience. Communication is accurate, succinct, timely and appropriate for the purpose and audience. Acts at all times with the highest levels of probity and honesty in their communications with colleagues, leaders, suppliers, auditors and the public.

Results focused

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

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

- Managing ICT security services and cyber security incidents in a comparable setting
- Achievement in a previous role of accredited security standards (Cyber Essentials +, ISO27001, NIST)
- Developing security policies and applying security principles
- Managing security in a SaaS / hybrid environment
- Creating technical and end-user documentation
- User education

Specific knowledge and skills

Several of the following:

- Network communications and architecture; endpoint, email and web configuration and security issues
- Current trends in cyber security: threats, tools and responses. Sources of current information and support on cyber security
- Change management processes
- MS Windows and Azure
- MS Defender
- ITIL
- GDPR
- Microsoft
- Qualified with AZ 500 or higher Microsoft qualifications, CISSP, CISM or CCSP, Security Administrator Associate or equivalent.
- SFIA Level 5