JOB DESCRIPTION

Job Title	Cyber Security Manager
Location	London
Mission	Medical Aid for Palestinians (MAP) works for the health and dignity of Palestinians living under occupation and as refugees. MAP is the leading UK charity delivering health and medical care to those worst affected by conflict, occupation, and displacement, in the occupied Palestinian territory and Lebanon
Hours	35 Hours per week
Reporting to	Head of Technology
Responsible for	n/a
Salary	£46,248
Key Internal relationships	IT Support Team, Internal Audit & Risk team
Key External relationships	All 3rd party IT vendors
Contract	Full-time, permanent

JOB PURPOSE

The Cyber Security Manager is responsible for protecting the organisation's digital assets and information systems from cyber threats. This role is central to developing, implementing, and managing a comprehensive cybersecurity strategy to safeguard data integrity, confidentiality, and availability. The Cyber Security Manager ensures the organisation's compliance with regulatory requirements, manages risk, and assist withs proactively identifying and mitigating security vulnerabilities and incidents. The primary goal is to reduce the likelihood and impact of cyber-attacks, ensuring the organisation can operate securely and without interruption.

MAIN RESPONSIBILITIES

Develop and Implement Security Policies:

- Design, implement, and maintain security policies, standards, and procedures in alignment with organisational goals and compliance requirements.
- Ensure adherence to industry best practices and regulatory standards (e.g., GDPR, HIPAA, PCI-DSS).

Manage Security Operations:

- Oversee the daily security operations, including monitoring and analysis of potential threats and vulnerabilities.
- Lead the deployment and management of security tools and technologies (e.g., firewalls, IDS/IPS, SIEM).

Incident Response and Management:

- Develop and maintain an incident response plan, coordinating with internal teams and external stakeholders to effectively respond to security incidents.
- Lead post-incident investigations, conduct root cause analysis, and implement corrective actions to prevent future breaches.

Risk Assessment and Mitigation:

- Conduct regular risk assessments and vulnerability assessments to identify security risks and develop mitigation strategies.
- Manage security audits and penetration testing to ensure continuous improvement of the security posture.

Training & Development:

- Plan and deliver cybersecurity training and awareness programs for staff, monitoring effectiveness of the program.
- Assist with upskilling the existing IT support team, fostering a culture of security awareness and continuous improvement.

Collaboration and Communication:

- Work closely with other departments (e.g., IT, compliance, legal) to ensure cybersecurity measures align with business objectives.
- Communicate security risks and strategies to senior management and stakeholders.

Stay Current with Threats and Trends:

- Keep up to date with emerging security threats, trends, and technologies to proactively enhance the organisation's security defenses.
- Engage with the cybersecurity community and participate in professional development opportunities.

SKILLS, EXPERIENCE & CANDIDATE ATTRIBUTES

Experience & Certifications/Qualifications:

- Relevant higher level qualification in computer science, Information Technology, Cybersecurity, or a related field; relevant certifications (e.g., CISSP, CISM, CEH) is preferred.
- Substantial demonstrable years of experience in cybersecurity and demonstrable experience of managing staff and operating at senior management level
- Strong knowledge of cybersecurity frameworks, technologies, and best practices.
- Experience with security tools such as SIEM, firewalls, IDS/IPS, antivirus software, and encryption solutions.
- Excellent problem-solving, analytical, and decision-making skills.
- Strong communication and leadership abilities.

Preferred Skills and Competencies:

- **Technical Proficiency:** Deep understanding of cybersecurity concepts, technologies, and tools.
- **Analytical Skills:** Ability to assess risks and identify vulnerabilities in the IT infrastructure.
- **Leadership Skills:** Capability to manage and inspire a cybersecurity team.
- **Communication Skills:** Strong ability to convey complex security issues to non-technical stakeholders.
- **Project Management:** Proficiency in managing multiple projects and priorities simultaneously.

Flexibility:

- On-call availability for responding to security incidents and to meet specific deadlines including some evenings and weekends.

Ethos:

- Support the mission & values of MAP.
- Support and promote diversity and equality of opportunity in the workplace.
- Represent and be an ambassador for MAP.
- Commitment to anti-discriminatory practice and equal opportunities.
- An ability to apply awareness of diversity issues to all areas of work.
- Abide by organisational policies, codes of conduct and practices.
- Commitment to upholding the rights of people facing disadvantage and discrimination.
- Commitment to a zero-tolerance policy on sexual exploitation & abuse/safeguarding.
- Able to work some evenings and weekends.

Other desirable experience:

- Experience of not-for-profit/INGO environments
- Experience with humanitarian issues, particularly those in Palestine.