IT SECURITY SPECIALIST



DIABETES UK
KNOW DIABETES. FIGHT DIABETES.

WHO WE ARE

We are Diabetes UK and it's our mission to tackle diabetes, day in and day out, until it can do no harm. One in five adults in the UK are living with diabetes or prediabetes, and we're determined to change that. Join us and together we can change the future of diabetes.

For the last 90 years, we've been behind vital policy changes, as well as new treatments and technologies to make living with diabetes easier every day. But there's more to do.

We're committed to preventing diabetes where possible, improving daily life for those living with it, and ultimately finding a cure. We're also focused on tackling stigma and reducing inequalities faced by people at risk or living with diabetes.

We've got some really ambitious goals over the next few years and we're looking for people who share our ambition to help us stop the harm diabetes causes.

We can't do any of this without you.

Our 2026 -2030 strategy commits us to 3 ambitious outcomes: Prevention and Cure, Everyone included and Living Well with Diabetes. To read more about our strategy please click here DUK-Strategy-2026-2030-compressed.pdf

At Diabetes UK, we live and breathe our values:

We put people first – We recognise that people are individuals with different preferences, circumstances and needs. We collaborate with others, listen carefully and keep commitments.

We make change happen – We are ambitious to drive change with and for people living with diabetes. We challenge constructively if needed.

We're driven to know more – We find ways to share knowledge and insights with colleagues and take advantage of learning opportunities across the charity.

We keep things simple – Diabetes is complicated enough.

If these values resonate with you, we'd love to hear from you.



Colette Marshall
Chief Executive

DIABETES UK
KNOW DIABETES. FIGHT DIABETES.

JOB DESCRIPTION

Role title: IT Security Specialist

Contract type: Permanent

Hours: 35 hours

Location: London

Salary: £41,035 - £51,000 – Band 5

Role reports to: IT Operations & Projects Manager

Key relationships (internal and external): IT Operations & Projects Manager, Infrastructure & Service Desk Lead, Information Governance, Data and Information Systems teams, Digital, IT Managed Service Providers, Security Operations Centre (SOC), external auditors and certification providers

Key focus of the role: The IT Security Specialist is Diabetes UK's experienced in-house technical security specialist, providing authoritative, hands-on information security expertise across the organisation. Working with a high degree of autonomy, the role owns key technical security processes, designs and implements proportionate controls, leads technical assurance, preventative and reactive response to significant cyber incidents, and provides oversight and constructive challenge to the Security Operations Centre and managed security providers. The postholder provides risk-based advice to projects, senior stakeholders and governance groups, ensuring services are secure by design and aligned with legal, regulatory and organisational requirements. Contributes to the ongoing improvement of the organisation's security maturity.

Key tasks and responsibilities

- Act as Diabetes UK's senior in-house technical security specialist and authoritative escalation point for security threats, vulnerabilities and incidents, exercising independent professional judgement and providing clear, risk-based advice.

- Develop, maintain and deliver a prioritised technical security improvement roadmap, translating organisational risks, audit findings, threat intelligence and regulatory requirements into proportionate and measurable actions.

- Design, implement, review and continually improve technical information security controls across Microsoft 365, Azure, endpoints, networks, cloud services and externally facing systems.

- Own the end-to-end technical vulnerability management process, including scanning coverage, risk-based prioritisation, remediation targets, exception management, escalation of overdue actions and verification of closure.

- Lead the technical coordination of significant cyber security incidents, working with the Security Operations Centre, managed service providers, Digital, Information Governance and senior stakeholders on triage, containment, recovery and post-incident improvement.

- Provide technical oversight and constructive challenge to the Security Operations Centre and managed security providers, reviewing service performance, alert quality, investigations, response times and completion of agreed remediation.

- Lead the technical delivery of Cyber Essentials Plus, PCI DSS and NHS Data Security and Protection Toolkit requirements, including control assessment, audits, evidence, assurance activity and remediation tracking.

- Lead technical security assurance for significant IT, digital and data projects, identifying requirements, assessing proposed solutions and recommending proportionate controls so that services are secure by design.

- Own designated information security processes and the security elements of the Diabetes UK IT Business Continuity Plan, testing their effectiveness and driving

continual improvement based on risks, incidents, exercises, audits and regulatory change.

- Coordinate scanning/ penetration testing and other technical assurance activity, assess findings and ensure responsible teams and suppliers complete agreed remediation within appropriate timescales.

- Prepare and present concise technical security reports, risk assessments, metrics and recommendations to the Information Governance Board and through the Keeping Safe, Legal & Healthy compliance risk management framework.

- Provide technical leadership, coaching and knowledge transfer to IT colleagues, and practical security guidance to staff and volunteers, helping to build a positive and proportionate security culture.

Person specification

	Criteria:		Assessed via:	
	E	D	A	I
Experience				
Significant hands-on experience in a technical cyber security role, including responsibility for making risk-based recommendations, owning security improvements and working with limited supervision.	X		X	X
Leading the technical delivery of security and compliance frameworks such as Cyber Essentials Plus, PCI DSS and the NHS Data Security and Protection Toolkit, including audit evidence and remediation.	X		X	X
Using Microsoft 365, Azure, Microsoft Defender XDR , Darktrace Purview and Microsoft Sentinel, or comparable SIEM and XDR platforms, to improve detection, response and compliance.	X		X	X
Applying information security management frameworks such as ISO 27001.	X		X	X
Developing technical security standards and processes, assessing control effectiveness and driving audit, risk and incident remediation.	X		X	X

	Criteria:		Assessed via:	
	E	D	A	I
Overseeing or constructively challenging an outsourced Security Operations Centre or managed security provider.		X	X	X
Knowledge				
Technical security architecture, control design and secure-by-design practices.	X		X	X
Data protection and information governance requirements.	X		X	X
Risk-based security decision-making, including vulnerability prioritisation, exceptions, compensating controls and escalation.	X		X	X
Leading or coordinating the technical response to significant cyber incidents and converting lessons learned into tracked improvements.	X			X
Skills				
Microsoft Defender XDR, Microsoft Sentinel, Purview & Darktrace or substantial transferable experience with comparable enterprise XDR and SIEM platforms.	X		X	X
Technical oversight of security monitoring and incident investigation delivered through a Security Operations Centre model.	X		X	X
Vulnerability management tooling, such as Qualys or equivalent.	X		X	X
Endpoint, network and cloud security controls.	X		X	X
Presenting technical risks, treatment options and recommendations clearly to senior stakeholders and governance groups.	X		X	X
Darktrace or comparable network detection and response tooling.		X	X	X
Qualifications/Professional membership (if applicable)				
Degree or equivalent experience in information security or IT.	X		X	
Relevant professional security qualification such as CISMP, CISM, CISA, CompTIA CySA+, Microsoft SC-200 or equivalent professional experience.		X	X	
Microsoft security certification such as SC-200 or AZ-500.		X	X	

	Criteria:		Assessed via:	
	E	D	A	I
Training or certification in Microsoft Sentinel, Microsoft Defender XDR, incident response or threat hunting.		X	X	

E – Essential D – Desirable A – Assessed at Application I – Assessed at Interview

If you don't meet all the criteria listed but meet most and have transferable skills with a passion for our mission, you are still welcome to apply for this role.

If you are invited to attend an interview in person, we will reimburse reasonable travel costs excluding hotel or overnight stays.

For candidates

All employees are expected to abide by our values and behaviours framework which can be found here Combined general and people managers framework. Below are a set of behaviours that you will be expected to demonstrate in your application form and that will also be explored during your interview.

Behaviours

We keep things simple

- Use clear, accessible language, avoiding jargon unless it's relevant to your audience.
- Design security controls and guidance that are clear, usable and sustainable.
- Explain technical risk in accessible language and make ownership and decisions clear.

We make change happen

- Speak confidently about the impact we've made and our ambitions for the future.
- Proactively seek solutions that strengthen security and remove obstacles to delivery.
- Take accountability for security decisions, actions and agreed improvements.

We're driven to know more

- Proactively look to learn more and share your new knowledge and insights with colleagues.
- Keep up to date with emerging threats and continuously develop professional expertise
- Seek and share insights, reflect on evidence and use learning to improve security practice.

We put people first

- Recognise that people are individuals with different preferences, circumstances and needs.
- Balance security requirements with the needs of staff, volunteers and people living with diabetes.
- Work collaboratively, assume positive intent and provide practical, respectful support.