Overview

Sector has been in business for 32 years contracting directly with NHS organisations. As a company we have grown technically with all major vendor operating systems and applications over this period, including Microsoft, VMware, Cisco, Oracle, HP and Opentext.

To ensure we deliver robust, reliable and consistent support to our customers, we follow the ITIL model of best-practice. We have a documented process, linking directly into problem management. Our Helpdesk Manager is responsible for ensuring that incidents are managed in line with the process and that problems are escalated to the senior technical team. The Helpdesk Manager retains end-to-end responsibility for all incidents to ensure satisfactory resolution.

Beyond the incident responses, we manage our customers' systems using formal change management, to minimise downtime and utilise routine monitoring processes to deliver capacity management as value-added services to our customers.

As experienced NHS providers data security and data integrity is at the heart of our provision. We are fully compliant and published for 24/25 with the NHS Data Security and Protection Toolkit. Our ODS code is RPGEL and can be used to confirm our status at www.dsptoolkit.co.uk. All staff completed the Data Security Awareness (NHSD), passing the associated tests. We have strict protocols for working with user data; any processing is undertaken in the trust's environments ensuring that we remain compliant with the Trust's data-processing standards. We never remove customer data from site.

All systems/services delivered by Sector have Cyber-Security built into their design and lifecycle management. New systems are built on the same customer-specific Gold-build OS templates ensuring consistency between servers and our on-boarding procedures ensure that cyber-security management processes, such as patch and security updates, are immediately integrated. Where systems are required to provide internet-facing services they are segregated from the production environment.

Sector manages every layer of IT service provision from hardware, LAN/WAN, virtual infrastructure, operating system and layered applications ensuring that cyber-security is not based on isolated systems but integral to every element of the service.

We work closely with our customers to analyse the impact of CareCerts from NHS-Digital and produce deployment and reconciliation plans where normal patching processes do not meet the requirements

We work in all aspects of the NHS including mental-health, acute hospital services, CCGs, GP and ICBs. We also contract within corporate and education markets enabling us to take best-practice models from all sectors. Our IT provision traverses all types of environments and enables us to bring this wealth of knowledge to all our customers as innovation, best-practice, improved service delivery and cost-savings. This breadth of skillsets makes us uniquely able to take a holistic approach to all aspects of our work particularly around problem management where we are able to bring skills even outside the core contractual offering to bear.

We offer a complete service provision which includes project management, systems design and specification, proof-of-concept, pilot deployments, production implementations, upgrades, patching, migrations and decommissioning. Our approach to building new systems or upgrading existing production servers is to build and test every process in a laboratory environment. Where live systems are being affected, we clone at a virtual machine level and isolate the environment to enable full process to be documented, tested and timed enabling our customers to produce full impact assessments on the production services and plan accordingly.

Sector manages our support operations in line with the principles set out in ISO27001. All our processes are developed and documented in a process specific PPG (Policy, Procedure, Guideline). The PPGs are entered into the

library once approved by a senior engineer and are available to all staff responsible for completing that procedure. PPGs may be specific to an organisation, product or both, and are reviewed at least annually, and during any upgrades or patches as part of the change-management process. The PPG library is secured so that only staff with the relevant skills to undertake the process can access them.

We take pride in delivering robust, flexible, scalable and cost-effective solutions at every layer of our provision. We are forward-thinking, adopting the latest, proven technologies; this coupled with our agile approach means with have the ability to react to our customers' needs.

Our range of skills already exceeds those required to deliver the future IT strategy set out in the tender – we understand IT strategies will adapt and develop and we welcome working with the Trust further advance IT strategy, leveraging our experience and knowledge to help the Trust develop.

Remote-support is a cost-effective way of delivering day-to-day services, however local, rapid on-site support remains essential to deliver on all aspects of our service – especially during time-critical situations when rapid response is vital.

Hybrid Cloud - Microsoft Server, Application & Infrastructure Support – Security Services

At Sector IT, we support NHS Trusts by delivering secure, resilient and fully managed hybrid cloud environments built around the Microsoft technology stack. By combining on-premises Microsoft Server infrastructure with Azure, Microsoft 365 and modern application services, we help organisations achieve the right balance between operational control, compliance and the agility required to support clinical services. Our approach ensures that NHS environments remain protected, available and aligned to national security standards while supporting the everyday needs of staff, clinicians and patients.

We work closely with NHS Trusts to develop a cohesive security strategy that unifies Active Directory, Azure AD, Microsoft 365, SharePoint, SQL, web services and remote-access platforms such as Always-On VPN. By adopting zero-trust principles, strong identity governance and Microsoft's advanced threat protection capabilities, we ensure that staff can securely access information whenever and wherever they need it. Using Power BI, we also provide consolidated visibility across servers, cloud resources and security events, giving Trust leadership meaningful data to support decisions around risk reduction and operational resilience.

Given the critical nature of NHS systems and the sensitivity of patient data, effective risk management is essential. We support Trusts with continuous monitoring and assessment across both on-premises and cloud infrastructure, using tools such as Defender for Cloud, SQL vulnerability assessments and Active Directory health reviews. Our risk-based approach identifies misconfigurations, insecure access paths and potential threat vectors before they can impact services. By ensuring Always-On VPN, Microsoft Server workloads and cloud applications are configured securely and remain fully patched, we help Trusts maintain compliance with NHS Digital, DSPT and wider regulatory obligations.

When designing hybrid cloud solutions for NHS organisations, we place security and continuity at the core of every architectural decision. This includes secure AD structures, RBAC, MFA, network segmentation and encrypted communication between on-premises and cloud environments. We design SQL, SharePoint, M365 and application services with robust access controls, high-availability capabilities and strong data protection measures. Azure-native technologies such as Key Vault, Sentinel and Defender are layered in to ensure that cryptographic keys, logs, identities and cloud resources remain protected and tamper-resistant. Our designs ensure not only resilience but seamless integration with existing NHS systems and workflows.

We provide NHS Trusts with structured incident management processes supported by automated detection and advanced security analytics. By combining Azure Sentinel, ATP, Microsoft 365 audit logs, server event monitoring and SQL auditing, we enable early detection of suspicious activity and coordinated incident response. Whether dealing with compromised accounts, malicious VPN activity, unauthorised access attempts or unusual cloud behaviour, we ensure rapid containment and thorough investigation. Following each incident, we support Trusts through remediation and post-incident improvement actions, strengthening their environment against future threats.

Features

UK based Service Desk (9am – 5.30pm)
On-premise or Cloud management services
Remote support services via HSCN or VPN
Enterprise solutions, scaled to your needs
Implemented with Cyber-Security at its core
New provisions, upgrades migrations for on-premise and cloud
System and Service Monitoring using Cloud or on-premise solutions
Microsoft Server, SQL, Always-on-VPN, Active Directory, Web Services, SharePoint, Microsoft 365, Azure, PowerBI, ATP

Benefits

Over 30 years of NHS experience
Working with NHS mental-health, acute hospital services, community services, GP and ICBs.
Free up your own staff to undertake more strategic work
Fully compliant and published for the NHS DSPT
Partnership focus to help drive value from your Microsoft investment
Workshops and visioning sessions to support knowledge sharing and understanding
Reduce sprawl: Upgrade, consolidate and reconcile existing systems