
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 we 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.

Cloud Networking – LAN and WAN Connectivity to Cloud - Cloud Migration Planning

At Sector IT, we begin every cloud networking engagement with a comprehensive capability analysis focused on the current LAN and WAN posture of the NHS Trust. This includes reviewing the Trust's utilisation of the Health and Social Care Network (HSCN), assessing bandwidth availability, resilience levels, routing configurations, and existing VPN infrastructure. We evaluate how well the network can support increased cloud demand such as Azure, AWS, or other hosted services while ensuring that clinical systems remain stable and responsive. Our analysis identifies whether the existing estate can support cloud migration at scale or whether specific upgrades are required in areas such as edge routing, segmentation, QoS, or security layers.

At an architecture level we map the interdependencies between on-premises systems, cloud platforms, HSCN connectivity, and internet-based access paths designing a cohesive architecture capable of supporting multi-cloud or hybrid-cloud operating models. This includes defining how LAN, WAN, and identity services align with cloud-based workloads and clinical applications. We make sure the architecture accommodates future digital initiatives, from virtual desktop platforms to clinical mobility programmes, while maintaining compliance with NHS network governance and security expectations.

We conduct a detailed cloud gap assessment to identify the readiness of the existing environment for cloud migration. This involves reviewing current routing design, DNS models, firewall configurations, address spaces, and endpoint dependencies that may influence or restrict cloud adoption. We also analyse gaps in resilience, security, monitoring capability, and network performance. For Trusts transitioning from an HSCN-centric model to combined HSCN and internet-based cloud access, we highlight where new controls, connectivity methods, or architectural adjustments are required. This assessment allows us to clearly define what must change to support safe, scalable, and compliant cloud networking.

Once the gaps are understood, we present a structured analysis of architectural options suited to NHS environments. This may include designs that retain HSCN as the primary connectivity path to specific services, options that introduce secure internet-based VPN connectivity to cloud platforms, or hybrid models using SD-WAN or multiple carriers for resilience. We evaluate each option in terms of security posture, operational complexity, cost, performance, compliance, and clinical impact. Our analysis helps Trusts make informed decisions about which architecture best supports their digital objectives, continuity requirements, and financial constraints.

To support successful adoption, we produce a clear delivery roadmap outlining how the Trust will transition from its current network state to the target cloud-enabled architecture. This roadmap includes sequencing of technical tasks, risk and dependency management, phased migration timelines, configuration updates, testing cycles, and operational handover planning. We ensure clinical services are protected by aligning migration activities with change governance,

peak operational periods, and Trust-specific service windows. The result is a practical, structured plan that guides the Trust through a safe, predictable, and well-governed cloud networking transition.

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
- Cisco, Aruba, Juniper, HSCN, Azure ExpressRoute, Azure VPN
- Fortinet, Sophos, Palo Alto

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
- Seamlessly Integrate network services into Azure Cloud Services
- On-premise to Cloud connectivity and service integration