
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 Endpoint Configuration Management – Managed Cloud

At Sector IT, we provide a fully managed Cloud Endpoint Configuration Management service designed specifically to support the complex and high-pressure environments within NHS Trusts. We understand that patient care relies on secure, reliable, and well-maintained clinical systems, and our service ensures that every endpoint across clinical, administrative, and remote settings are consistently configured and operating safely. By centralising endpoint management across private, public, and hybrid cloud platforms, we help Trusts maintain a stable digital foundation that supports clinical workflows and improves service delivery.

In NHS environments, application availability and performance are critical. Our service places application management at the forefront, ensuring that essential software is securely packaged, deployed, updated, and monitored across all cloud models. Whether your Trust relies on on-premises datacentres, Azure-hosted workloads, or hybrid cloud configurations, we ensure seamless and consistent application delivery. This reduces downtime, minimises disruption to clinical teams, and helps ensure staff always have timely access to the tools they depend on.

We recognise that cybersecurity and regulatory compliance are paramount within NHS organisations. Our managed service aligns with NHS Digital guidance, national cybersecurity frameworks, and Information Governance requirements. We enforce standardised policies, secure configurations, and rigorous application patching across your endpoint estate to protect sensitive patient data and maintain operational continuity. Through continuous monitoring and proactive remediation, we identify and address vulnerabilities before they can impact clinical systems, supporting your Trust's resilience and compliance efforts.

NHS Trusts often operate a diverse technology landscape, combining legacy on-premises solutions with modern cloud-based services. Our endpoint configuration management service is designed to operate seamlessly across private, public, and hybrid cloud environments, ensuring consistent application delivery regardless of where systems are hosted. Whether supporting digital transformation programmes, modernising legacy applications, or integrating new cloud services, we provide a flexible management framework that aligns with your Trust's infrastructure strategy and digital maturity roadmap.

Our service not only improves the reliability and security of devices and applications but also supports wider NHS digital objectives. By automating routine tasks, standardising configurations, and simplifying the entire application lifecycle, we reduce operational burden on internal IT teams and enable them to focus on transformation and patient-centred innovation. At Sector IT, we are committed to delivering a scalable, resilient, and future-ready endpoint management service that strengthens digital infrastructure across your Trust and contributes to safer, more efficient patient care.

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
Datto, MECM, ZCM, Intune, Avanti, ENGL
Software deployment, patching, remote control, imaging, security configuration
ATP, reporting, cyber security

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 on-premise hardware investments and costs for backup storage
Fully managed backup solution
Meet your cyber security requirements for DSPT
Fully managed service