
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 – Security Services

At Sector IT, we embed a strong security strategy into every aspect of our Cloud Endpoint Configuration Management service, ensuring NHS Trusts have a resilient and well-governed approach to protecting their endpoint estate. Our strategy is shaped around NHS-specific frameworks, including national cyber guidance, Data Security and Protection Toolkit expectations, and the operational realities of clinical environments. We focus on establishing clear security baselines, maintaining consistent controls across private, public, and hybrid cloud platforms, and ensuring endpoints are configured to safeguard patient data while supporting uninterrupted clinical workflows.

We recognise that unmanaged security risks can directly impact patient care, operational continuity, and regulatory compliance. Our approach to security risk management involves continuous assessment of endpoint configurations, application behaviours, cloud interactions, and the evolving threat landscape. We identify weaknesses such as configuration drift, unpatched software, legacy dependencies, or elevated-privilege misuse, and put remedial plans in place before they lead to incidents. By maintaining a strong understanding of NHS risk categories, escalation routes, and governance requirements, we help Trusts mitigate security threats in a structured, clinically aware manner.

Security design is a core component of our service. We implement secure-by-design principles throughout the endpoint lifecycle, ensuring devices, applications, policies, and cloud-based configurations are architected with protection and resilience built in from the start. This includes hardening standards, role-based access controls, automated policy enforcement, and secure application deployment pipelines. Whether endpoints are managed via public cloud platforms like Microsoft Intune, on-premises solutions, or a hybrid model, we design configurations that uphold NHS security requirements while enabling mobility, flexibility, and modern digital ways of working.

In the event of a security incident, rapid and coordinated action is essential. We provide a structured incident management capability that enables NHS Trusts to contain, analyse, and resolve endpoint-related security events efficiently. This includes monitoring for anomalous behaviour, investigating endpoint or application-level compromises, isolating affected devices through cloud management tools, and supporting recovery activities. We work closely with Trust cybersecurity teams, following established NHS escalation procedures and contributing forensic insights where required. Our focus is to minimise disruption to clinical services and support a swift return to normal operations with lessons learned fully captured.

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