
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.

Hybrid Cloud Data Migration – Security Services

At Sector IT, we help develop security strategies that ensure cloud data migrations are delivered safely, consistently, and in full alignment with NHS governance expectations. Our strategies establish how data will be protected as it moves between on-premises systems and cloud platforms, defining the controls, assurance measures, and monitoring tools required throughout the migration lifecycle. We embed NHS cyber guidance, zero-trust principles, and patient data safeguarding requirements into every stage of planning. This allows Trusts to adopt cloud capabilities with confidence, knowing that risk, compliance, and clinical safety remain central to the migration approach.

Cloud migrations introduce new risk areas from data-in-transit exposure to authentication model changes and we manage these risks proactively and transparently. We assess vulnerabilities across existing infrastructure, cloud platforms, identity services, and data flows to understand where exposures may arise. Our security risk management process considers clinical dependencies, service uptime requirements, legacy system constraints, and regulatory obligations. By identifying risks early and developing mitigation plans that align with NHS operational requirements, we help Trusts minimise disruption and ensure that migrated data remains secure, available, and compliant.

Security design is a core component of our cloud migration services. We create architectures that ensure data encryption, identity governance, network segmentation, and access controls are consistently applied across all environments on-premises, private cloud, and public cloud. Our designs incorporate secure migration pipelines, controlled access boundaries, hardened storage configurations, and event-level monitoring that spans the entire estate. Whether the Trust is adopting Azure, AWS, or a hybrid model, we ensure that security controls are integrated from the outset, supporting both resilience and long-term digital scalability.

In a cloud environment, incidents can originate from multiple layers network, identity, data movement tools, endpoint access, or cloud services. We deliver a coordinated security incident management capability that monitors activity across the entire migration landscape. If suspicious behaviour or a security breach is detected, we work with NHS cyber teams to isolate affected components, protect data, and restore normal operation. We support detailed investigation, root-cause analysis, and evidence gathering while ensuring clinical services remain operational throughout. Our approach ensures that Trusts are equipped to respond quickly, confidently, and safely to any incident during or after migration.

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
Micro Focus OES, ZCM, Vibe, Filr, IDM
Preserve existing configuration and security models
Translate Novell/Micro Focus/Open text ACLs into equivalent Microsoft Models

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
Meet your cyber security requirements for DSPT
Fully managed service and migrations