
Sector IT - 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 Backup Services – Security Services

Modern IT security services play a critical role in protecting both cloud-based and on-premise backup environments. As organizations generate more data than ever, the need for secure, reliable, and compliant backup solutions has become essential. Here at Sector IT, we focus on safeguarding data throughout its entire lifecycle, during transfer, storage, and recovery using advanced encryption, access controls, monitoring, and automated threat detection.

A strong security strategy underpins these efforts, ensuring that every layer of protection aligns with business goals and the DSPT requirements. By incorporating security risk management practices, we can identify vulnerabilities, assess potential threats, and prioritize remediation efforts to reduce exposure. These measures together help ensure that sensitive information remains protected from cyberattacks, insider threats, and accidental loss.

In hybrid environments where cloud and on-premise systems coexist, IT security services provide an integrated approach to resilience. Cloud backups offer scalability, rapid deployment, and geographic redundancy, while on-premise backups give NHS Trusts tighter controls, lower latency, and additional layers of protection.

Effective security risk management is a foundational component of modern IT security services, ensuring that Trusts can proactively identify, assess, and mitigate potential threats before they impact operations. This involves continuous evaluation of backup environments, both cloud-based and on-premise, to detect vulnerabilities, misconfigurations, or emerging risks that could compromise data integrity. Through structured risk assessments, threat modelling, and regular compliance reviews, Sector IT helps your IT teams gain a clear understanding of where the greatest exposures lie. These insights enable the development of targeted controls, prioritise remediation plans and long-term strategies that reduce overall risk. By embedding risk management into everyday processes, Trusts not only strengthen their security posture but also improve resiliency and readiness in the face of evolving cyber threats.

Strong security design is essential for building resilient backup environments that can withstand modern threats while supporting operational needs. This involves architecting systems with security embedded from the start, including network segmentation, least-privilege access models, encryption standards, and automated policy enforcement. In both cloud and on-premise infrastructures, well-designed security controls ensure that data protection mechanisms are consistent, scalable, and aligned with industry best practices. Security design also incorporates redundancy, fault tolerance, and validated recovery workflows, ensuring that backups remain intact and recoverable even under adverse conditions. By adopting a security-by-design approach, we help Trusts create a solid foundation that reduces vulnerabilities, improves maintainability, and strengthens their overall security posture.

Effective security incident management is crucial for minimizing the impact of disruptions and ensuring rapid recovery when security events occur. This process includes continuous monitoring, timely detection of anomalies, and coordinated response efforts to contain and remediate threats across both cloud and on-premise backup

environments. Sector IT can assist local Incident management teams with predefined playbooks, forensic analysis, and automated alerting to quickly identify root causes and prevent further damage. Regular testing, such as tabletop exercises and recovery drills, ensure that response procedures remain efficient and aligned with evolving threats. By maintaining a mature incident management capability, NHS Trusts can reduce downtime, preserve data integrity, and maintain confidence in their overall security and backup strategies.

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
- On-premise backup to cloud integration
- Veeam, VMware, Physical and Virtual machines, immutability, archive
- Disaster Recovery, Business Continuity

Benefits

- Over 30 years of NHS experience
- 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
- Backup on-premise and cloud workloads