WHITE PAPER

IGEL: Supporting NHS Data Security &Protection Toolkit (DSPT) endpoint self-assessment

As the NHS continues to evolve its digital landscape, compliance with the Data Security and Protection Toolkit (DSPT) becomes increasingly time consuming and difficult. By eliminating some of the reporting requirements and streamlining endpoint security, IGEL can help reduce the impact of annual compliance reporting while reducing the potential for cyber-attacks each and every day. This solution brief outlines how IGEL's technology can empower NHS organisations to enhance data security, streamline endpoint management and contribute to meeting the stringent requirements of the DSPT.

Delivering security for healthcare now and next

The NHS faces unique challenges in managing and securing its critical clinical endpoints. Key challenges include:

- **Fast, simple, yet secure access to patient information:** Clinicians need instant access to a patient's latest information – potentially while dealing with multiple critical situations such as in an A&E setting. Technology must be supportive, not distracting.
- **Data security and privacy:** Protecting sensitive patient information is critical, necessitating robust measures to prevent data breaches and unauthorised access.
- **Endpoint diversity:** The NHS operates a wide range of endpoint devices, creating complexity in standardization and security.
- **Budget:** As with any publicly funded institution, IT budget concerns limit innovation and are often consumed with "keeping the lights on" – ensuring existing systems remain operational.

IGEL's endpoint strategy for healthcare now and next enables NHS Trusts and Integrated Care Board (ICB) Management to deliver secure, cloud-based digital workspaces that support delivery of patient care, reduce breaches, and optimise IT budgets.

IGEL's transformative Preventative Security Model supports Zero Trust security initiatives and eliminates vulnerable endpoint attack vectors. Reduced attack surface, modular design, no local data, and a read-only OS eliminates the need for costly, complex security agents.

IGEL partners with essential care delivery peripheral manufacturers and platform providers to support microphones, signature pads, badge-tap technologies, EMR workflows and other critical clinical and administrative functions.

How IGEL Addresses DSPT Compliance:

IGEL works with more than 40 NHS Trusts to deliver improved security, reduced costs and fast access to patient information.

v5 22-23 Evidence reference	Evidence Text - NHS Trusts and CSUs	How IGEL can help
1.1.4	Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	The IGEL Management Console provides asset data on every IGEL endpoint. This data can be exported to a single asset management tool or view. Management of user access and roles is provisioned through the UMS/IGEL Cloud Services management consoles.
1.3.1	There are board-approved data security and protection policies in place that follow relevant guidance.	IGEL supports security and data protection policies through the IGEL Preventative Security Model™. No data is stored at the endpoint and the IGEL is read-only removing common attack vectors
1.3.2	Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.	IGEL Insight Service collects analytical and usage data from all users to improve analysis, reporting, security and optimization
1.3.6	List your organisation's top three data security and protection risks.	IGEL can help mitigate and prevent security risks such as ransomware and malware using the IGEL Preventative Security Model.
1.3.7	Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.	IGEL can mitigate and prevent security risks using the IGEL Preventative Security Model.
1.3.11	If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	IGEL supports BYOD use cases using the IGEL UD Pocket which enables the secure use of BYOD devices – without using its local OS. Access is provided through IGEL OS like any other corporate device. USB storage access is locked down by default, but customisable as required.
1.4.3	If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?	No data is ever stored locally on the IGEL device removing the need for secure destruction
4.1.2	Users in your organisation are only given the minimum access to sensitive information or systems necessary for their role.	IGEL supports least privileged access - through access to applications. For example, IGEL devices will only display Citrix/VMWare/Microsoft AVD applications that the end-user has access too. IGEL Universal Management Suite fully supports RBAC.
4.2.1	When was the last audit of user accounts with access to the organisation's systems held?	IGEL Universal Management Suite fully supports RBAC. IGEL devices fully integrate into an organisations existing authentication system (such as Microsoft Entra ID) and therefore supports an organisation's access permissions.
4.2.3	Logs are retained for a sufficient period, managed securely, reviewed regularly, and can be searched to identify malicious activity.	IGEL Universal Management Suite supports logging of administrative management actions with no minimum data retention period. Logs can be exported to 3rd party data analysis tools and incorporated into standard policies and procedures

v5 22-23 Evidence reference	Evidence Text - NHS Trusts and CSUs	How IGEL can help
4.2.4	Unnecessary user accounts are removed or disabled.	IGEL fully integrates with Microsoft Active Directory and therefore supports the removal of unnecessary accounts. IGEL devices can be removed and disabled from the Universal Management Suite console as required.
4.3.2	Users, systems and (where appropriate) devices are identified and authenticated prior to being permitted access to information or systems.	With IGEL SSO, users must authenticate prior to accessing applications. With regards to NLA (NDES/SCEP), the devices must be authenticated before network access is permitted.
4.4.3	The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation	Through 3rd party partner integrations such as Systrack and Control Up, user interaction can be monitored. Remote access/shadowing of users can be carried out with the permission of the user
4.5.3	Multifactor authentication is used wherever technically feasible.	With IGEL OS, we support multifactor authentication as well as SSO solutions (Microsoft Entra ID, Okta, Imprivata, Ping) We can also use MFA built into client access solutions – > Citrix, VMware Horizon and Microsoft AVD/365
6.2.1	Antivirus/anti-malware software has been installed on all computers that are connected to or are capable of connecting to the Internet.	IGEL's Preventative Security removes the vulnerabilities targeted by bad actors. Although there is no requirement to install AV on IGEL OS, AV can be installed if required for tracking / reporting
6.2.3	Antivirus/anti-malware is kept continually up to date.	IGEL's Preventative Security removes the vulnerabilities targeted by bad actors. Although there is no requirement to install AV on IGEL OS, AV can be installed if required for tracking / reporting
6.2.4	Antivirus/anti-malware software scans files automatically upon access.	IGEL's Preventative Security removes the vulnerabilities targeted by bad actors. Although there is no requirement to install AV on IGEL OS, AV can be installed if required for tracking / reporting
6.2.5	Connections to malicious websites on the Internet are prevented.	IGEL OS integrated browser has configurable restrictions and controls.
8.1.1	Provide evidence of how the organisation tracks and records all software assets and their configuration.	IGEL OS can report on what software is installed on each IGEL endpoint.
8.3.1	How do your systems receive updates and how often?	IGEL Universal Management Suite manages the updating of all IGEL OS endpoints centrally. For the IGEL OS, we release updates every 1 - 2 months unless there are critical security issues where we can provision OS updates as required. IGEL applications receive updates as necessary through the IGEL App Portal.
8.3.2	How often, in days, is automatic patching typically being pushed out to remote endpoints?	We can automatically roll out updates as and when they come available in line with App and or OS updates release schedule.
8.3.7	95% of your organisation's server estate and 98% of your desktop estate are on supported versions of operating systems.	With IGEL OS license structure, as long as you have active maintenance, you will be allowed to update to the latest version of IGEL OS to maintain support.

v5 22-23 Evidence reference	Evidence Text - NHS Trusts and CSUs	How IGEL can help
8.4.1	Your organisation's infrastructure is protected from common cyber-attacks through secure configuration and patching?	Both IGEL Universal Management Suite and IGEL OS are patched as soon as a risk is identified, and a CVE published. IGEL's Preventative Security Model eliminates many of endpoint vulnerabilities commonly targeted by attackers.
9.3.6	The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption.	All data configuration and updates traveling between the Management Suite and the Device are encrypted.
9.3.8	The organisation maintains a register of medical devices connected to its network.	Using IGEL Asset Inventory Tracker, IGEL can list devices that are connected to the endpoint allowing us to track peripherals.
9.5.1	All devices in your organisation have technical controls that manage the installation of software on the device.	IGEL has an App Portal where applications can be downloaded to the Universal Management Suite and then rolled out to endpoints. End users are not able to install any software that has not already been sanctioned by your organisation.
9.5.2	Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.	Using the Universal Management Suite, IGEL can remotely reset the device back to factory defaults. The OS is read-only, and relevant configuration / data partitions are encrypted.
9.5.5	End user devices are built from a consistent and approved base image.	The base IGEL OS image across all devices is the same image managed from the Universal Management Suite, however, applications rolled out to each device may differ depending on use case.
9.5.6	End user device security settings are managed and deployed centrally.	This is done all configured through the Universal Management Suite.
9.5.7	Autorun is disabled.	Users cannot have application autorun unless this is specifically initiated via the Universal Management Suite
9.5.8	All remote access is authenticated.	This can be done via the Universal Management Suite using Secure VNC
9.6.6	All of your organisation's desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default.	With IGEL OS, any unapproved port connection is denied.
10.2.1	Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	IGEL does not handle or process patient or staff information.

For more information please contact – NHS@IGEL.com

For more information or to register for trial access,
please visit www.igel.com/get-started/try-for-free.

Visit us at igel.com

IGEL