2026 DSPT Version 8 – GP Category 4 Statement

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?***
Data on hard drives and solid-state drives on from the GPIT Infrastructure are destroyed by Pure Planet Recycling Ltd who hold ISO14001 certification and shred data storage media while at ITS Digital's premises. Shredding evidence is checked by ITS Digital and signed off before they leave site with the waste for recycling.

4.3.1 ***Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?***
Yes, all system administrators have signed an agreement which holds them accountable to the highest standards of use.

4.4.1 ***The person with responsibility for IT confirms that IT administrator activities are logged, and those logs are only accessible to appropriate personnel.***
Confirmed. ITS Digital ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel.
Privileged accounts are reviewed regularly, and processes exists where the Server Teams are alerted to any changes to these accounts.
Server Logs are held on an in-house management tool.
Network logs are held in-cloud behind MFA and PIM.
Logs cannot be tampered with by end users.

4.5.3 ***Multi-factor authentication is used on all remotely accessible user accounts on all systems, with exceptions only as approved by a relevant board or senior management.***
All remote systems (VPN, VDI) require the user to have active MFA before allowing access.

4.5.4 ***How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?.***
All systems have a password complexity requirements and staff are informed of password best practices.

7.1.1 ***Do you have a digital asset register detailing your organisation's hardware and software, which is kept up to date?***
Confirmed for all GPIT assets.

7.1.6 ***Assets (hardware, software and data) are owned and managed throughout their lifecycle.***
We can confirm that all obsolete devices are identified, securely disposed and replaced as appropriate. We have a process that ensures that any assets that are re-used, transferred or disposed of are recorded in the asset register. We can confirm that software is managed through its lifecycle and decommissioned when appropriate.

8.1.2 Does the organisation track and record all end user devices and removable media assets?
Confirmed for GPIT supported data assets (desktop PCs, laptops, servers) that a centralised asset register is held. Removable media is blocked by default and a separate exceptions list is held and approved by management.

8.1.4 Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?
Confirmed for GPIT related software and systems.

8.3.1 How do you make sure that the latest software updates are downloaded and installed promptly?
We deploy updates at the earliest opportunity after Microsoft publishes them and they have been tested. We deploy daily deployment for AV updates and for other systems upgrades as and when advised by suppliers if not applied automatically. The GPIT infrastructure is monitored via MDE, which provides real-time security monitoring, advanced threat detection, vulnerability management and automated investigation & response, amongst others.

8.3.2 How often, in days, is automatic patching typically being pushed out to remote endpoints?
We deploy updates at the earliest opportunity after Microsoft publishes them and they have been tested. We deploy daily deployment for AV updates and for other systems upgrades as and when advised by suppliers if not applied automatically. The GPIT infrastructure is monitored via MDE, which provides real-time security monitoring, advanced threat detection, vulnerability management and automated investigation & response, amongst others.

8.3.5 How does your organisation make sure that the latest software updates are downloaded and installed promptly?
We deploy updates at the earliest opportunity after Microsoft publishes them and they have been tested. We deploy daily deployment for AV updates and for other systems upgrades as and when advised by suppliers if not applied automatically. The GPIT infrastructure is monitored via MDE, which provides real-time security monitoring, advanced threat detection, vulnerability management and automated investigation & response, amongst others.

8.3.8 Your organisation is registered for and actively using the NCSC early warning service.
Not required. The GPIT infrastructure is monitored via MDE, which provides very thorough protection from both an endpoint and network scanning perspective, with comprehensive malware detection that is overseen by a national NHS team, as well as end point software integrated into the operating system and managed by GPO. NHS England's Cyber Security Operations Centre (CSOC) monitors for new threats and attacker activity 24 hours a day, 7 days a week, providing real-time protection – we also utilise the CSOC Secure Boundary service, which uses next generation firewall (NGFW) and web application firewall (WAF) protection to protect internet traffic from digital and cloud-based threats.
MDE and CSOC services provide real-time monitoring and protection, whereas the NCSC early warning system simply provides details of potential cyber issues gathered from a variety of cyber threat intelligence feeds, all of which already part of the MDE and CSOC services already in use.

8.4.1 Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?
Confirmed for the managed GPIT infrastructure.

8.4.2 All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.
Confirmed for the managed GPIT infrastructure.

8.4.3 You identify and understand security vulnerabilities in your systems, such as through regular vulnerability testing.
Confirmed for the managed GPIT infrastructure.

9.3.1 All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.
Approved applications are assessed for common security vulnerabilities and are patched/removed as applicable.

9.3.4 The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.
Confirmed.

9.3.5 The organisation understands and records all IP ranges in use across the organisation.
Confirmed.

9.4.4 Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.
Confirmed.

9.5.1 All devices in your organisation have technical controls that manage the installation of software on the device.
Confirmed.

9.5.2 Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?
Confirmed that all laptops and tablets supported on the GP IT infrastructure are encrypted. We employ port control to prevent data being copied to removable media.

9.5.3 You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.
Confirmed.

10.2.1 Do your organisation's IT system suppliers have cyber security certification?
ITS Digital currently hold CE+ certification (certificate number 5d9380af-d3e6-499b-a8b3-1da03d2c80af) and Data Security and Protection Toolkit (Version 7 - standards exceeded).