Northern Health and Social Care Trust

FOI 3749

Technology Procurement

Please provide the following information.

1. Please provide the record from the organisations Contract Register or equivalent procurement log entry pertaining to the current contract for the Endpoint Detection and Response (EDR) solution (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used]).

DEFINITION: The practice of securing organisational assets such as laptops, desktops, mobile phones, and servers against malicious activity. It encompasses tools and strategies designed to detect, prevent, and respond to threats directly on the device itself.

See response and the exemption and public interest test below.

2. Please provide the following information for the current maintenance and licensing agreement for the primary Perimeter Firewall/Intrusion Prevention System (IPS) solution (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used]).

DEFINITION: The processes and technologies used to protect the boundaries (the perimeter) of an organisations internal network from unauthorised external access. It involves monitoring and controlling incoming and outgoing network traffic.

See response and the exemption and public interest test below.

3. Please provide the following information for the service agreement covering the Cloud Security Posture Management (CSPM) platform or equivalent third-party cloud security monitoring too (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used]).

DEFINITION: The set of security measures designed to protect data, applications, and infrastructure running in cloud environments (e.g., AWS, Azure, GCP). It also includes securing internally and externally facing applications themselves (application security).

See response and the exemption and public interest test below.

4. Please provide the following information for the service agreement covering your Identity & Access Management (IAM) software (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used]).

DEFINITION: A framework of policies and technologies that ensures the right users have the appropriate access to the right resources at the right time. It involves managing digital identities, authentication (verifying identity), and authorisation (granting access).

See response and the exemption and public interest test below.

5. Please provide the record from the organisations Contract Register or equivalent procurement log entry pertaining to the current contract for your current Managed Security / SOC Services (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used])

DEFINITION: The outsourcing of security monitoring and management to a third-party expert. A Security Operations Center (SOC) is a centralised function (internal or outsourced) responsible for continuous monitoring, threat analysis, and managing security incidents.

See response and the exemption and public interest test below.

6. Please provide the record from the organisations Contract Register or equivalent procurement log entry pertaining to the current contract for your current Vulnerability & Compliance Management service (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used])

DEFINITION: The continuous, cyclical practice of identifying, classifying, prioritising, remediating, and mitigating software weaknesses (vulnerabilities). Compliance Management ensures that security practices adhere to specific internal policies, regulatory requirements (like GDPR), and industry standards.

See response and the exemption and public interest test below.

Exemption and Public Interest Test

The Trust is mindful that any disclosure of information under FOI legislation is to the world at large and not just to the person who submitted the request. This has been taken into account when deciding on the release of information in response to an FOI request, giving due consideration to the exemptions preventing disclosure of certain information into the public domain.

The Trust has feels that this information meets the requirement for exemption under Section 43 (Disclosure would pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the NHSCT relies).

In order to engage the exemption, the Trust must demonstrate that there is a causal link between the endangerment and disclosure of the information and that disclosure would or would be likely to have, a significant threat to the integrity and operation of the digital systems on which the day to day business of NHSCT relies. The threat cannot be trivial or insignificant.

In recent years, there have been a number of Cyber Attacks on public authorities, where the perpetrators may have exploited vulnerabilities in ICT systems and software to gain access and either deploy ransomware or steal information. In May 2021 the Health Service in Ireland (HSE) suffered such an attack and in light of this, the Trust is mindful that by releasing information about the digital infrastructure and devices connected to its ICT network (which may also be electronically linked to other healthcare organisations in Northern Ireland), it could reveal versions of systems/software/quantities/contacts which may be exploitable and would enable access to its wider ICT network.

This would endanger the information it holds on patients, clients and staff and the loss of this information would directly impact on the physical or mental health wellbeing of those patients and clients, as the Trust would not have access to key information for continuity of their care. Given the potential for a ransomware or other Cyber related attack, the actual risk of a remote attack on the Trust's ICT network is real, substantial and probable.

For this reason the Trust will not be releasing details of the Trust's specific Cyber investment and Cyber vendors/technology solutions or brands as has been requested within this FOI request as this has the potential to increase the likelihood for a remote attack on our ICT systems.

Section 43 – Public Interest Test

Section 43 is a qualified exemption. This means that, as information requested is exempt from disclosure, the Trust consider and then decide whether the public interest in maintaining the exemption outweighs the public interest in its disclosure. In the case of section 43 this involves weighing up the threat to the integrity & operation of the digital systems on which the day-to-day

business of the NHSCT relies and the potential impact on health and safety to patients, clients and staff against any public interest in disclosure.

The assessment of endangerment is relevant to this public interest test as the Trust believes this information would be of use to perpetrators and the impact of such an attack would be substantially detrimental for our patients and clients. Due to the level and likelihood of endangerment, the Trust is convinced there is a very strong public interest in not disclosing the information requested and the Section 43 exemption is fully engaged.

EXEMPTION CLAIMED IN RESPECT OF SECTION 43 **Integrity & operation of the digital systems**	
In favour of disclosure of information	**In favour of maintaining exemption and not disclosing information**
The Trust's desire for openness, fairness, transparency and equity.	There have been a number of cyber-attacks against health care and public sector organisations across the UK and ROI, which demonstrates a strong risk to the NHSCT's ICT Systems.
Transparency in accountability of public funds and ensure public money is being used effectively. Provide assistance to the public in understanding where and how public monies are spent.	The Trust holds highly sensitive information on our patients and clients and the loss (even temporarily) of this information would impact on the Trust's ability to deliver services and provide medical and social care.
To ensure procurements and contracts are conducted and managed in an open and honest way.	There would be a detrimental impact on the mental health and wellbeing of our clients (and patients) if their data was compromised or stolen.
Ensuring there is competition for public sector contracts.	The Trust may be liable to regulatory action or a monetary penalty if information was released into the public domain (via FOIA) which

	contributed to identifying vulnerabilities in our ICT systems and ultimately led to or contributed to remote cyber-attack.
	Release of the information in light of the potential impact may undermine public confidence in the Trust.
	A potential cyber-attack will endanger the Trust's wider ICT systems, further compromising its ability to deliver services.
	A Cyber-attack may impact upon other health trusts who use the same regional systems and place supplier/contracting organisations at risk.