

1 April 2026

Contract Register / Equivalent Procurement Log Entry Pertaining to Contract for Endpoint Detection and Response (EDR) Solution

QUESTIONS:

1. Please provide the record from the organisation's 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.*
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 organisation's internal network from unauthorised external access. It involves monitoring and controlling incoming and outgoing network traffic.*
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 tool (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).*
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).*

1 April 2026

5. Please provide the record from the organisation's 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 Centre (SOC) is a centralised function (internal or outsourced) responsible for continuous monitoring, threat analysis, and managing security incidents.*
6. Please provide the record from the organisation's 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.*

BELFAST HEALTH AND SOCIAL CARE TRUST RESPONSE

Belfast Trust has considered each requested data field individually and in combination. While certain items may appear low risk when viewed in isolation, the request seeks consistent categories of information across multiple, core cyber security control layers. Disclosure of these fields in aggregate would create a detailed intelligence picture of the Trust's defensive posture, supplier ecosystem, and operational timing. This aggregated disclosure would materially increase cyber security risk by reducing the effort required for hostile reconnaissance and enabling more targeted and effective cyber-enabled criminal activity.

The Trust confirms that it holds information relating to contractual arrangements for cyber security services across Digital Services. To meet transparency and public assurance objectives, the Trust is disclosing confirmation that appropriate cyber security contracts are in place, together with a single aggregated annual spend figure for Digital Services.

Disclosed information:

2024/2025 Aggregated Annual Spend for Digital Services: £16,337,432

Belfast Trust is withholding supplier names, product details, contract dates, procurement routes, system-level spend, and operational notes under Sections 31(1)(a) and 38 of the Freedom of Information Act 2000, as detailed below.

1 April 2026

Key

Outcome	Disclose / Withhold
Rationale	Summary rationale for exemption which intentionally avoids disclosure of information that could increase cyber risk
Exemption	Section 31(1)(a) – Prevention or detection of crime (cyber-enabled crime) Section 38 – Health and safety (risk to individuals arising from cyber incidents)
Items	1. Endpoint Detection & Response (EDR) 2. Perimeter Firewall / IPS 3. Cloud Security Posture Management / Cloud Monitoring 4. Identity and Access Management 5. Managed Security / SOC Services 6. Vulnerability and Compliance Management

Items 1–6: Core Cyber Security Contracts

Element Requested	Outcome	Rationale	Exemption ¹
Confirmation contracts exist	Disclose	Meets transparency and public assurance objectives without revealing actionable detail	N/A
Supplier name	Withhold	Disclosure would enable threat actors to identify the Trust's cyber security supply chain, correlate it with known vulnerabilities, supplier-specific advisories, or active attack campaigns, and increase the likelihood of targeted compromise or supply-chain attack, particularly when combined with other disclosed fields	S31(1)(a), S38

¹ S31 applies where crime prevention is directly prejudiced. S38 applies where the **foreseeable consequence** of that prejudice is a risk to individuals

1 April 2026

Product name	Withhold	Reveals specific defensive technologies in use, enabling attackers to research product-specific weaknesses, evasion techniques, and exploit pathways. Aggregated across multiple control layers, this significantly reduces attacker reconnaissance effort	S31(1)(a), S38
Contract start / expiry dates	Withhold	May indicate periods of renewal, transition, or system change during which operational focus may be divided or controls reconfigured. Such timing information can be exploited to increase attack success rates	S31(1)(a)
Framework / procurement route	Withhold	Discloses supplier ecosystem relationships and procurement patterns that can inform targeting and social-engineering activity	S31(1)(a)
System-level annual spend	Withhold (system-level) Disclose (aggregated)	A single aggregated annual spend figure for Digital Services is disclosed to support transparency. Disclosure of system-level or control-specific spend would reveal relative investment priorities and potential defensive strengths or weaknesses that could be exploited	S31(1)(a)
Additional notes / service detail	Withhold	Contains operational context and service detail with high reconnaissance value, supporting targeted phishing, social engineering, or lateral attack planning	S31(1)(a), S38

These exemptions are Qualified Exemptions and are therefore subject to a Public Interest Test (PIT).

I can confirm that we have carried out a PIT and the outcome is to maintain the exemptions and withhold the information from release.