Reference:	FOI.19593.26
Subject:	Contract Register/Procurement logs
Date of Request:	12 February 2026

Requested:

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 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).

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).

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 Center (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.

Response:

Hywel Dda University Health Board (UHB) has applied an exemption under Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA) to the supplier and product names as it has deemed that the information requested is exempt from disclosure as it would be likely to prejudice the prevention or detection of crime and potentially increase the risk of cyber-crime. The UHB has also considered the "mosaic effect"; the harm which will or will be likely to arise from the release of this information, when utilised alongside information already in the public domain.

Section 31 of FoIA is a qualified exemption requiring public authorities to apply the public interest test set out in Section 2(2)(b).

The information can only be withheld if the public interest in maintaining the exemption outweighs the public interest in disclosure.

The UHB has therefore considered the following:

In favour of disclosure: The UHB has a duty to maintain openness and transparency in all its activities, including decision making, which will help to maintain public trust in the UHB. Disclosing cyber security product information could provide assurance to the public that the UHB has a robust IT infrastructure in place, which in turn would reassure the public that their information is safe, and that public money has been well spent to ensure this.

Against Disclosure: A disclosure made under the FoIA, is a disclosure to the world at large and by releasing the supplier and product names, the UHB would be vulnerable to it being used for crime. Such action could compromise the security of UHB systems and both patient and staff information, whilst causing disruption to the flow of information through the UHB systems, impacting on patient care and safety.

The UHB takes its Data Protection and Information Governance responsibilities very seriously and has robust arrangements in place to protect its IT systems and infrastructure. Disclosure of this information would reveal how to undermine systems, with the potential need to implement disproportionate steps resulting in additional expense to the public purse, to counter an increased risk that is currently managed.

Decision: Disclosing the information regarding the UHB's cyber security products will likely provide attackers with valuable information regarding the capability of the UHB's cyber security. Such a disclosure would enable targeted research that would compromise the integrity and confidentiality of its systems which contain sensitive information. The UHB has also taken into account the wider context of significant and growing cyber threats and attacks which continue to present a substantial risk to the world at large.

There is a clear public interest in protecting society and the UHB from the impact of crime. Therefore, the UHB has concluded that the public interest in withholding the supplier and product

names is greater than the interest in disclosing, consequently protecting the UHB from potential criminal activity.

1. The UHB provides within the table below, the information requested relating to its Endpoint Detection and Response (EDR) solution.

Supplier	Section 31 exemption applied
Product Name	
Start Date	29 December 2024
Expiry Date	28 December 2027
2025/26 annual spend	£148,467.00 as part of a wider contract
Framework	NPS-ICT-0094-19

2. The UHB provides within the table below, the information requested relating to its four (4) maintenance and licensing agreements for its Perimeter Firewall/Intrusion Prevention System (IPS) solutions.

Supplier	Section 31 exemption applied			
Product Name				
Start Date	1 August 2025	1 April 2025	14 September 2025	1 March 2024
Expiry Date	31 July 2026	31 March 2026	30 April 2027	28 February 2029
2025/26 annual spend	£29,950.60	£19,200.00	£1,971.60	£62,953.08
Framework	SBS/19/AB/WAB/9411			

3. The UHB's Cloud Security Posture Management (CSPM) platform is incorporated into its ESR solution agreement. Therefore, please see response to question 1.

4. The UHB does not hold the requested information, the Service Level Agreement (SLA) agreement for its Identity and Access Management (IAM) software is managed by Digital Health and Care Wales (DHCW). We therefore recommend that you re-direct this part of your request to the Freedom of Information (FoI) Team in DHCW, who should be able to help you with your enquiry.

Contact details are as follows:
DHCW.FOI@wales.nhs.uk or alternatively in writing to: Digital Health and Care Wales, Ty Glan-yr-Afon, 21 Cowbridge Road East, Cardiff, CF11 9AD.

5. The UHB's Security Information and Event Management Services (SIEM) are incorporated into its ESR solution agreement. Therefore, please see response to question 1. Additionally, the UHB also pays £40,839.00 annually to DHCW via a Service Level Agreement for an all NHS Wales SIEM.

6. The UHB provides within the table below, the information requested relating to its two (2) vulnerability and compliance management services.

Supplier	Section 31 exemption applied	
Product Name		
Start Date	1 March 2024	1 February 2024
Expiry Date	1 March 2027	31 January 2027
2025/26 annual spend	£3,164.16	£55,844.64
Framework	NPS-ICT-0094-19	SBS/19/AB/WAB/9411