Mersey and West Lancashire Teaching Hospitals NHS Trust

Ref. No:	1803
Date:	04/06/25
Subject:	Contracts for Firewall, Anti-virus, Microsoft Enterprise Agreement, and Power BI

REQUEST

1. Standard Firewall (Network)

Firewall services that protect the organisation's network from unauthorised access and other internet security threats.

2. Anti-virus Software Application

Programs designed to prevent, detect, and remove viruses, malware, trojans, adware, and related threats.

3. Microsoft Enterprise Agreement

A volume licensing agreement that may include:

- Microsoft 365 (Office, Exchange, SharePoint, Teams)
- Windows Enterprise
- Enterprise Mobility + Security (EMS)
- Azure services (committed or pay-as-you-go)

4. Microsoft Power BI

Or any alternative business intelligence platform used for data connectivity, dashboards, and reporting.

For each of the above areas, I kindly request the following:

1. Who is the existing supplier for this contract?
2. What is the annual spend for each contract?
3. What is the description of the services provided?

4. Primary brand (where applicable)
5. What is the start date of the contract?
6. What is the expiry date of the contract?
7. What is the total duration of the contract?
8. Who is the responsible contract officer?
   • Please include **at least their job title**, and where possible, **name, contact number, and direct email address**
9. How many licences or users are included (where applicable)?

Important Notes

- I **do not request** any technical specifications such as device models, serial numbers, IP ranges, or site-level infrastructure details that may pose a security or operational risk.
- If full disclosure of named personnel is not possible under Section 40 of the FOI Act, I would still appreciate disclosure of **job titles and generic contact information**, such as a team inbox or switchboard extension.
- If any commercial sensitivities under Section 43 apply, I respectfully request a **clear explanation of the specific harm** expected from disclosing aggregated annual spend or supplier names, especially where the contract has already been awarded.
- This request is made in line with the principles of the **Procurement Act 2023**, which reinforces the importance of transparency and public access to contract information, particularly around supplier identity, contract value, and duration.

RESPONSE

Standard Firewall

- Security Risk: Disclosing details about firewall services could reveal the type, configuration, or vendor used, which may help attackers identify vulnerabilities or tailor attacks.

- Exemption Justification: Under many FOI laws (e.g., UK FOIA Section 31), information can be withheld if disclosure would likely prejudice the prevention or detection of crime.

Anti-virus Software Application

- Security Risk: Revealing the specific antivirus software in use may allow attackers to exploit known weaknesses or test malware against that software.
- Exemption Justification: This information could compromise the effectiveness of our malware defence strategy, making the organization more vulnerable to cyberattacks.

Microsoft Enterprise Agreement

- Security Risk: While licensing details may seem administrative, they can indirectly reveal the scope of software in use, which could help attackers understand our digital environment.
- Exemption Justification: If the agreement includes sensitive details about deployment or security features (e.g., EMS or Azure configurations), it could be used to map your infrastructure.

Microsoft Power BI or Alternatives

- Security Risk: Disclosing the business intelligence platform in use could expose potential attack vectors, especially if the platform is integrated with sensitive data sources.
- Exemption Justification: Knowledge of internal reporting tools and data connectivity methods could aid in social engineering or data exfiltration attempts.

Summary of Exemption Grounds

- Risk of facilitating cyberattacks (e.g., phishing, malware, unauthorized access).
- Prejudice to law enforcement or crime prevention.
- Protection of internal systems and data integrity.

The application of Section 31(1)(a) of the Freedom of Information Act is justified in cases where the disclosure of specific contractual and technical details could undermine the security of an organisation and expose it to malicious threats. Publicly revealing the contract supplier of fireworks, along with details such as contract length and cost, creates potential IT security risks by exposing both the supplier and contracting organisation to cyber threats, social engineering attacks, and financial exploitation. Malicious actors could use this information to craft phishing scams, impersonate the supplier,

or manipulate contract negotiations for fraudulent purposes. Revealing contract length enables attackers to anticipate renewal cycles, increasing susceptibility to fraudulent bids and misinformation campaigns, while disclosing contract costs exposes financial details that may be exploited for targeted cyber-attacks.

Similarly, making antivirus details publicly available compromises the Trust's cybersecurity posture by revealing its defence mechanisms, leaving it vulnerable to cyber threats, hacking attempts, and malware infiltration. Attackers could exploit disclosed information, such as software versions, update schedules, and configuration settings, to design malware capable of bypassing security measures. Additionally, employees may be manipulated through phishing scams to disable or alter security protocols. Furthermore, revealing financial and contractual information related to antivirus solutions could lead to fraudulent vendor activities, misinformation campaigns, or targeted financial exploitation, thereby increasing IT security risks.

Equally, the public disclosure of Business Intelligence (BI) dashboard details presents significant security concerns by exposing data analytics, reporting structures, and strategic insights to unauthorised individuals. Cybercriminals could leverage this information to manipulate reports, exploit weaknesses in data governance, or gain insights into internal decision-making processes. Revealing dashboard configurations, user access permissions, and integration points with other systems can facilitate unauthorised access and increase the likelihood of phishing attacks targeting privileged users. Additionally, financial, and contractual information regarding BI solutions could be exploited by fraudulent vendors or used to craft misinformation campaigns, further compromising organisational security.

Section 31(1)(a) of the FOIA is applied to protect the security and integrity of organisations by restricting the disclosure of information that could be exploited for criminal activities. Withholding details regarding suppliers, cybersecurity measures, and BI dashboard configurations is essential to mitigating risks, preventing unauthorised access, and safeguarding financial and operational security