

Resolution

8th Floor,
10 South Colonnade
Canary Wharf
London
E14 4PU

Telephone: 020 7811 2700

July 2025

FOI_7253

The following information was requested on 4 June 2025:

I am conducting a research project into how public sector organisations procure cyber security services and enterprise software platforms. As part of this, I would be grateful if you could provide the most recent contract information you hold for the following areas:

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)?*

Our Response

1. Standard Firewall (Network)

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

NHSR Response: We do have firewall in place; however, we are unable to disclose further details on the grounds of cyber security. This information is withheld for crime prevention reasons. Section 31 of the Freedom of Information Act 2000 is applicable. Please see the refusal notice below.

2. Anti-virus Software Application

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

NHSR Response: We do have software in place; however, we are unable to disclose further details on the grounds of cyber security. This information is withheld for crime prevention reasons. Section 31 of the Freedom of Information Act 2000 is applicable. Please see the refusal notice below.

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)*

NHSR Response: We have an MS Enterprise agreement in place covering our licensing. In addition, we have a Cloud Service Provider contract in place for Azure Services.

4. Microsoft Power BI

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

NHSR Response: We have MS Power BI in place as part of our licensing agreement.

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

NHS Response – applicable to points 3 and 4 above for Microsoft Licensing

1. *Who is the existing supplier for this contract?*
 - Trustmarque
2. *What is the annual spend for each contract?*
 - Annual spend for 24/25 – £707,441 excluding VAT
3. *What is the description of the services provided?*
 - The licences we hold within the agreement includes
 - AzureDevOpsServe
 - M365 E5 Original Sub
 - Power Virtual Agent Sub
 - Power Virtual Agent USL
 - Project P3
 - Visio P2

- Visual Studio Ent with GitHub
- Win RDS CAL
- AzureDevOpsServe
- M365 E5 Original Sub
- Teams AC with Dial Out US/CA Sub Add-on
- Power Virtual Agent
- Power Virtual Agent USL Sub
- Project P3
- Visio P2
- Visual Studio Ent with GitHub
- Win RDS CAL
- Power Automate Sub

SCE

- CIS Suite Datacentre core
- CIS Suite Standard core
- SQL Server Ent Core
- SQL Server Std Core

4. *Primary brand (where applicable)*
 - Microsoft
5. *What is the start date of the contract?*
 - 01/02/2023
6. *What is the expiry date of the contract?*
 - 31/01/2026
7. *What is the total duration of the contract?*
 - 3 years
8. *Who is the responsible contract officer?*
 - Please include at least their job title, and where possible, name, contact number, and direct email address
 - Head of Service Operations, Amit Panchal, amit.panchal@nhs.net
9. *How many licences or users are included (where applicable)?*
 - Licence volumes based on requirements will vary however we are working across 920 users.

NHS Response – applicable to point 3 – Azure Cloud Service Provider

1. *Who is the existing supplier for this contract?*
 - ANS
2. *What is the annual spend for each contract?*
 - Annual spend for 24/25 – £378,278 excluding VAT
3. *What is the description of the services provided?*
 - Managed Cloud Service Provider for Azure environment
4. *Primary brand (where applicable)*
 - Microsoft

5. *What is the start date of the contract?*
 - 25/10/2022
6. *What is the expiry date of the contract?*
 - 25/10/2025
7. *What is the total duration of the contract?*
 - 3 years
8. *Who is the responsible contract officer?*
 - *Please include at least their job title, and where possible, name, contact number, and direct email address*
 - Head of Service Operations, Amit Panchal, amit.panchal@nhs.net
9. *How many licences or users are included (where applicable)?*
 - Not applicable

Refusal notice for Q1 & Q2 – Section 31 – Law Enforcement

We consider that disclosing the details of our Firewall and the Anti-virus software we use would be likely to increase the risk of successful attempts to hack our network. The information could be used by any person in the world (as is the nature of a disclosure under FOIA), particularly in conjunction with other information about our systems, to plan or prepare more sophisticated attacks. Section 31(1) of the FOI Act applies to this information.

31(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice – (a) the prevention or detection of crime.

Public Interest Test

Public Interest considerations in disclosing the information

There is a general public interest in openness and transparency in public sector bodies which can help to maintain public trust. Information relating to NHS Resolution's IT operating systems are clearly matters of public interest. We recognise that there is a legitimate interest in knowing what systems we utilise, which helps to promote public confidence that the organisation maintains high levels of security.

Public interest considerations in favour of maintaining the exemption

NHS Resolution recognises its duty to protect personal data held on our systems, as disclosure will, in our opinion, weaken our ability to protect our stakeholders. Disclosing the information requested would mean releasing details about our systems and their security into the public domain. This could make the information accessible to criminals, by enhancing criminals' abilities to carry out cyber-attacks. It also follows that

risk to our systems will also constitute a risk to both the general public and NHS Resolution staff whose information we hold.

By withholding this information, criminals will be prevented from exploiting such information in order to target our systems or individuals.

Balance of Public Interest Test (PIT)

NHS Resolution acknowledges that there is an interest in the public knowing that the organisation has adequate levels of protection in place for its IT systems, to ensure that we mitigate any risks befalling our systems on which we rely to run the organisation. We believe that ensuring the safety of our systems is paramount and on the balance of the PIT, we believe that there would be a clear causative link in disclosing the information you have requested which could expose the organisation to the risk of crime and subsequently endanger or cause harm to those whose data we hold. NHS Resolution therefore believes that the greater public interest in withholding this information.

This concludes our response to your request.

If you are not satisfied with the service that you have received in response to your information request, it is open to you to make a complaint and request a formal review of our decisions. If you choose to do this, you should write to [Joanne Appleby](#), Deputy Data Protection Officer for NHS Resolution, within 28 days of your receipt of this reply. Reviews of decisions made in relation to information requests are carried out by a person who was not involved in the original decision-making about the request.

If you are not content with the outcome of your complaint, you may apply directly to the Information Commissioner for a review of the decision. Generally, the Information Commissioner will not make a decision unless you have exhausted the local complaints procedure. The address of the Information Commissioner's Office is:

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

<https://ico.org.uk/>