Request for information under the Freedom of Information Act Reference 2021.901
Released 26 October 2021

Thank you for your email received 29 September 2021 requesting information regarding ITSM.

Please find detailed below a summary of your request, together with our response.

Summary of your original request:
Please could you provide details of the following:

If there is more than one solution, please provide details for each

1. What is your current end point patching solution? e.g. SCCM/WSUS/Solarwinds/ManageEngine etc(appreciate you may not divulge this for Cyber security reasons)

Releasing the name of our end point patching solution could compromise the security of the system. This information is therefore exempt under Sections 31(1) Prevention and Detection of Crime and 24(1) National Security of the Freedom of Information Act 2000 (the FOIA). Disclosure of this information would be likely to both prejudice law enforcement and increase the vulnerability of the Trust, which could ultimately aid potential attackers.

Prejudice
Providing details of systems used may lead to the Trust being vulnerable to a cyber-attack. This information could aid attackers in selecting targets, thereby increasing the vulnerability of public authorities. The Trust believes that this would prejudice both the prevention and detection of cybercrime and national security. NHS organisations including the Trust hold large amounts of personal, sensitive and confidential data and there is a considerable public interest in protecting NHS organisations' systems from potential cyberattack.

Both Sections 31(1) and 24(1) are prejudice based exemptions and subject to a public interest test. This means that not only does the information have to prejudice one of the purposes listed, but before the information can be withheld, the public interest in preventing that prejudice must outweigh the public interest in disclosure.

Public Interest Test

Considerations in favour of disclosure:

- The inherent public interest in the openness and transparency of public authority dealings

Considerations against disclosure:

- Disclosing this information could expose the IT security systems of the Trust to the risk of a targeted attack

- Disclosing this information would increase the vulnerability of specific NHS organisations on a national level leading to the disruption of NHS organisations' ability to conduct business
- Disclosing this information could aid an attacker by highlighting areas or organisations that could be more vulnerable to attack than others
- Applying this exemption will prevent the disclosure of information that would facilitate or encourage criminal activity
- A successful attack would have a direct impact on patient care

Conclusion:
The Trust recognises that there is a public interest in the disclosure of information which facilitates the accountability and transparency of public bodies for decisions taken by them. However, there is also a public interest in the security of information held by the Trust which is put to the wider public interest.

Having undertaken the balancing exercise, the Trust has concluded that the public interest in maintaining the exemption significantly outweighs the public interest in disclosing the requested information. Particular weight has been placed on the severity of the prejudice which may be caused were the Trust to release the names of some products used.

Given that the definition of 'public' under the Act is considered to be the public at large, rather than just the individual applicant or a small group of people and that 'public interest' is not necessarily the same as what interests the public, it is considered that to release this information is likely to result in prejudice to the security systems of NHS organisations including the Trust which is not outweighed by the wider public interest for disclosure.

The Information Commissioner's Office (ICO) has confirmed that they consider that the safeguarding of national security also includes protecting potential targets even if there is no evidence that an attack is imminent. In recent months there have been published vulnerabilities against NHS organisations, including the very significant incident in May 2017. The Trust considers that the greater public interest lies with the security of the type of information held by them and that of third parties. In the Trust's opinion, the additional risk to clinical data held by the Trust and the impact a successful attack would have on direct patient care means disclosure cannot be justified.

Is it cloud / on-premise / hybrid?

On premise

What is your current end point patching solution contract start date and end date?

June 2016 to June 2021

Did you complete a competitive process for the procurement of this?

Yes

Will you complete a competitive process for the procurement of a new solution?
If so, which framework?
If not, what are the reasons?

Yes, a competitive process will be followed for procurement of a new solution. At this stage, no decision has been made as to which framework will be used.

What is the cost of the existing solution?

£61,500

What budgets are in place for future solutions

The budgets for future solutions has not yet been decided.

2. What is your current IT service desk solution? e.g. ServiceNOW, ZenDesk etc

Top Desk

Is it cloud / on-premise / hybrid?

On-premise

What is your current IT service desk solution contract start date and end date?

04/04/21 – 04/04/24

Did you complete a competitive process for the procurement of this?

No. An extension clause in the existing contract was enacted.

Will you complete a competitive process for the procurement of a new solution?
If so, which framework?
If not, what are the reasons?

We do not hold any information in relation to the procurement of a new solution, as no decisions surrounding this have been made yet.

3. What is your current remote device management solution? E.g. BeyondTrust Remote support, RDS, Teamviewer,VNC,Zoho Assist, AnyDesk etc.

Releasing the name of our remote device management solution could compromise the security of the system. This information is therefore exempt under Sections 31(1) Prevention and Detection of Crime and 24(1) National Security of the Freedom of Information Act 2000 (the FOIA). Disclosure of this information would be likely to both prejudice law enforcement and increase the vulnerability of the Trust, which could ultimately aid potential attackers. Please see refer to the public interest test carried out under question 1 above.

Is it cloud / on-premise / hybrid?

On-premise

What is your current remote device management   solution contract start date and end date?

No contract date for this solution.

Did you complete a competitive process for the procurement of this?

No.

Will you complete a competitive process for the procurement of a new solution?
If so, which framework?
If not, what are the reasons?

We do not hold any information in relation to the procurement of a new solution, as no decisions surrounding this have been made yet.

4. Do you have a Digital Employee Experience solution and what is it? (e.g. NextThink, Digital Experience Cloud, Kadiska DEX)

No.

Is it cloud / on-premise / hybrid?

N/A

What is your current solution contract start date and end date?

N/A

Did you complete a competitive process for the procurement of this?

N/A

Will you complete a competitive process for the procurement of a new solution?
If so, which framework?
If not, what are the reasons?

N/A

5. Do you have a SIEM and what is it? (e.g. Splunk/MS Sentinal) Do you have central Log collector and what is it? (e.g. Graylog) , LogStash etc.) Is it cloud / on-premise / hybrid?

Releasing the name of our central log collector solution could compromise the security of the system. This information is therefore exempt under Sections 31(1) Prevention and Detection of Crime and 24(1) National Security of the Freedom of Information Act 2000 (the FOIA). Disclosure of this information would be likely to both prejudice law enforcement and increase the vulnerability of the Trust, which could ultimately aid potential attackers. Please see refer to the public interest test carried out under question 1 above.

What is your current solution contract start date and end date?

We do not hold any information in relation to the procurement of this solution, as no decisions surrounding this have been made yet.

Did you complete a competitive process for the procurement of this?

Yes, a competitive process was completed for this contract.

Will you complete a competitive process for the procurement of a new solution?
If so, which framework?
If not, what are the reasons?

We do not hold any information in relation to the procurement of a new solution, as no decisions surrounding this have been made yet.

6. Do you have a SNMP monitoring solution and what is it? (e.g. Solarwinds)

Releasing the name of our SNMP monitoring solution could compromise the security of the system. This information is therefore exempt under Sections 31(1) Prevention and Detection of Crime and 24(1) National Security of the Freedom of Information Act 2000 (the FOIA). Disclosure of this information would be likely to both prejudice law enforcement and increase the vulnerability of the Trust, which could ultimately aid potential attackers. Please see refer to the public interest test carried out under question 1 above.

Is it cloud / on-premise / hybrid?

On-premise

What is your current solution contract start date and end date?

Sept 21 – Sept 22

Did you complete a competitive process for the procurement of this?

No.

Will you complete a competitive process for the procurement of a new solution?
If so, which framework?
If not, what are the reasons?

We do not hold any information in relation to the procurement of a new solution, as no decisions surrounding this have been made yet.

***7. Do you outsource any ITSM components?
If so, which?***

No

***Do you outsource any Cyber Security components?
If so, which?***

No