FOI 0264/2023 Request

1. **What was the total number of cyber-attack incidents that have been recorded in your trust in the past 24 months?**

0

2. What is the classification of your policy regarding breach response?

Classification is based on the nature of the breach.

The Trust do have in place a cyber incident response plan and this includes classification policy.

3. Of the devices running Windows operating systems, what is the number and percentage of devices running Windows 11, Windows 10, Windows 7, Windows XP?

100% Windows 10 and Approx. 4900 devices.

4. What are the top 20 cyber security risks in your Trust, and how are they managed?

The Trust is unable to provide a response to this query.

This is because disclosure of the requested information may create vulnerabilities to the Trust's ICT security and leave our servers vulnerable to cyber-attacks.

The Trust therefore, rely on exemption Section 24 of the Freedom of Information Act 2000 to deny this aspect of your request.

5. Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed.

The Trust currently is not using Unified Cyber Risk Framework.

6. What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows , Windows XP)?

The Trust Patch management cycle is monthly and in accordance with Microsoft Tuesday patching.

Please note that there is no XP and Win 7 OS in use.

7. What is your current status on unpatched Operating Systems?

Disabled until updated.

8. Of the devices running Windows Servers operating systems, what is the number and percentage of devices running Windows 2000, Windows 2003, Windows 2008, Windows 2012, Windows 2016,

The Trust is unable to provide a response to this query.

This is because disclosure of the requested information may create vulnerabilities to the Trust's ICT security and leave our servers vulnerable to cyber-attacks.

The Trust therefore, rely on exemption Section 24 of the Freedom of Information Act 2000 to deny this aspect of your request.

9. Has your Trust signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience? If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation?

Yes, the Trust has signed up to and implemented the NHS Secure Boundary managed service to strengthen our cyber resilience.

Please note that there have been no threats.

10. Does your Trust hold a cyber insurance policy? If so:

a. What is the name of the provider.

b. How much does the service cost; and

c. By how much has the price of the service increased year-to-year over the last three years?

The Trust is unable to provide a response to this query.

This is because disclosure of the requested information may create vulnerabilities to the Trust's ICT security and leave our servers vulnerable to cyber-attacks.

The Trust therefore, rely on exemption Section 24 of the Freedom of Information Act 2000 to deny this aspect of your request.

11. When did the current Board last receive a briefing on cybersecurity threats within healthcare, and when did they last participate in cyber security training? How frequently, if at all, do these briefings and trainings occur, and are they carried out by cyber security technology professionals?

Quarterly updates are reported and annual cyber and Information governance training is deployed Trust wide.

12. Has your NHS Trust completed a Connection Agreement to use the Health and Social Care Network (HSCN)? If so, did you pass, and is there a copy of the code of connection?

We are part of HSCN and have been using the connection for the last few years.

13. Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance?

No.

14. How many open vacancies for cyber security positions are there within your Trust, and is their hour capacity affected by a shortage of qualified applicants?

There are currently no vacancies and the Trust is not affected by the shortage.

15. Are there mandatory minimum training requirements for those transferred internally to work in cybersecurity within your Trust, and if so, how often is the training updated and revised to reflect the evolving nature of the industry?

As part of annual mandatory training for all staff. Reviewed and updated annually.

16. How much money is spent by your Trust per year on public relations related to cyber-attacks? What percentage of your overall budget does this amount to?

The Trust is unable to provide a response to this query.

This is because we do not capture isolated costs for cyber-attacks publication**.**

17. Does your Trust have a Chief Information Risk Officer? If so, who do they report to?

Yes, the Trust has a Chief Information Risk Officer and a Senior Information Risk Owner.

Both report to the CEO.

18. When was the last time your Trust underwent a security audit? At what frequency do these audits occur?

A security audit took place in 2022 and this is done annually.

19. What is your strategy to ensure security in cloud computing?

We follow NHS Digital and NHS England guidance to secure all systems including Cloud hosted systems.

20. Do you purchase additional / enhanced support from a Supplier for end-of-life software (Operating Systems / Applications)? If so, what are the associated costs per year per Operating System /Application, and the total spend for enhanced support?

The Trust is unable to provide a response to this query.

This is because disclosure of the requested information may create vulnerabilities to the Trust's ICT security and leave our servers vulnerable to cyber-attacks.

The Trust therefore, rely on exemption Section 24 of the Freedom of Information Act 2000 to deny this aspect of your request.