FOI 1931

Date 19/01/2023

Dear Requester,

Thank you for your Freedom of Information request. Please note, this is a cross-site response for Bedford site and Luton site.

You asked:

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

Section 31(1) - This question is exempt under Section 31(1) Information is exempt if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime. It could be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures and it is the view of this Trust that the disclosure of the requested information would prejudice our ability to resist cyber-attacks on our systems.

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

Based on NCSC’s Classification

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

This question is exempt under Section 31(1)

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

This question is exempt under Section 31(1)

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

Yes: 11

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

This question is exempt under Section 31(1)

1. **What is your current status on unpatched Operating Systems?**

This question is exempt under Section 31(1)

1. **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, Windows 2019, Windows 2022?**

This question is exempt under Section 31(1)

1. **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: This information is available from provided by NHS Secure Boundary

1. **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?**

This question is exempt under Section 31(1)

1. **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?**

Sept 2022. Training is by NCSC approved provider

1. **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?**

Yes: Yes.

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

No

1. **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?**

2

1. **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?**

Yes. As often as required

1. **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?**

**Public Relations is handled by Communications Dept.**

This question is exempt under Section 31(1)

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

Yes: To the CEO

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

This question is exempt under Section 31(1)

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

Follow NCSC’s Guideline on Cloud Security

1. **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?**

This question is exempt under Section 31(1)

This information is provided for your personal use and is the property of Bedfordshire Hospitals NHS Trust and subject to any existing Intellectual Property and Database Rights. Any commercial application or use of this information may be subject to the provisions of the Re-use of Public Sector Information Regulations 2015 (RPSI). This means that if you wish to re-use the information provided for commercial purposes for any reason you must ask the Trust for permission to do so.

Please note that the Trust has a formal internal review and complaints process which is managed by the Information Governance Manager/Data Protection Officer. Should you have any concerns with our response, you can make a formal request for an internal review. Requests for internal review should be submitted within three months of the date of receipt of the response to your original letter, and should be addressed to: dataprotectionofficer@ldh.nhs.uk. This option is available to you for up to three calendar months from the date your response was issued.

If you are not satisfied with the Trust review under the Freedom of Information Act 2000 you may apply directly to the Information Commissioners Officer (ICO) for a review of your appeal decision. The ICO can be contacted at: ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF www.ico.org.uk

Yours sincerely,

*FOI Officer*

Bedfordshire Hospitals NHS Foundation Trust