Freedom of Information Request	FOI 23-033	10th February 2023

I am writing to you to request the following information about your NHS Trust under section 1(1) of the Freedom of Information Act 2000:

1. **What was the total number of cyber attack incidents that have been recorded in your trust in the past 24 months?**
   The Health Board has been the subject of 1 Cyber attack reportable under regulatory requirements.

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

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?**
   I can confirm that the Health Board holds information that you have requested. However, the Health Board believes that releasing this detailed information creates a security risk and is likely to prejudice the prevention or detection of crime (section 31(1)(a)) so in this case we will not be providing it to you as it is exempt from disclosure.

   In line with the terms of this exemption in the Freedom of Information Act, we have also considered whether it would be in the public interest for us to provide you with the information, despite the exemption being applicable. In this case, we have concluded that the public interest favours withholding the information.

4. **What are the top 20 cyber security risks in your Trust, and how are they managed?**
   All risks are managed using the Health Board's risk framework.
   Please refer to Q3.

5. **Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed.**
   Please refer to Q3.

6. **What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows , Windows XP)?**
   Please refer to Q3.

7. **What is your current status on unpatched Operating Systems?**
   Please refer to Q3.

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, Windows 2019, Windows 2022?
Please refer to Q3.

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?**
   None.

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?
    NHS Wales insurance is provided by the Welsh Risk Pool which covers all potential insurance liabilities. There are no specific costs associated with cyber insurance policies. You would need to contact the Welsh Risk Pool direct to obtain this information.

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?**
    The Board have engaged with a Cyber Security consultancy and security briefings and training has been provided during the last 12 months. Individual Board members are also receiving specialised training to support their security roles.

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?**
    The Health Board is connected to the NHS Wales Network.

13. **Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance**
    None.

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?**
    The Health Board currently has one Cyber Security related position advertised and are therefore unable to comment as the recruitment process is still ongoing.

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?**

External or internal applicants must meet qualification and knowledge requirements for the position. Additional training is provided to maintain/enhance the skills of the Cyber Team. This is provided annually through training courses and mentoring.

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?**
    None.

17. **Does your Trust have a Chief Information Risk Officer? If so, who do they report to?**
    No. The Health Board has a Senior Information Risk Owner (SIRO) who reports to the Board.

18. **When was the last time your Trust underwent a security audit? At what frequency do these audits occur?**
    The Health Board is subject to scheduled annual security audits

19. **What is your strategy to ensure security in cloud computing?**
    The Health Board's strategy is aligned to the Cyber Security Centre Cloud Security Guidance as follows: Cloud security guidance - NCSC.GOV.UK

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?**
    No.