

From: Freedom of Information

Sent: 29 October 2020 16:06

To:

Subject: Freedom of Information Response (Our Ref: K/20/403)

Dear

Freedom of Information Response (Our Ref: K/20/403)

Thank you for your Freedom of Information (FOI) request dated 15 October 2020, reference K/20/403.

Your request read:

“SECURITY / CYBERSECURITY:

What SEIM (Security Event and Incident Management) solution is used by your organisation?

When does your SEIM (Security Event and Incident Management) platform license subscription come up for renewal?

If the SEIM (Security Event and Incident Management) solution was purchased via third party please disclose the contracting party's details?

Do you outsource your security management to a third party (managed security service provider)? If so can you disclose the name of the managed security service provider.

When does the current service contract from the current managed security service provider end?

Can you provide the email address of the individual that is responsible for your IT Security?

ICO - breaches:

How many cyber security breaches has your organisation had over the past 2 yrs?”

The University of Leeds holds some of this information.

For your convenience, we have provided answers to each of your questions in turn below.

- 1. What SEIM (Security Event and Incident Management) solution is used by your organisation?**

Splunk

- 2. When does your SEIM (Security Event and Incident Management) platform license subscription come up for renewal?**

October 2021

- 3. If the SEIM (Security Event and Incident Management) solution was purchased via third party please disclose the contracting party's details?**

Softcat

- 4. Do you outsource your security management to a third party (managed security service provider)? If so can you disclose the name of the managed security service provider.**

We do not outsource our security management.

- 5. When does the current service contract from the current managed security service provider end?**

N/A

- 6. Can you provide the email address of the individual that is responsible for your IT Security?**

No single individual is responsible for IT security.

- 7. How many cyber security breaches has your organisation had over the past 2 yrs?**

We have been subject to attempted cyber-attacks in the previous two years. Where required, we report breaches to the Information Commissioner's Office (ICO).

However, we consider that further details are exempt from disclosure under section 31(1)(a) of the Freedom of Information Act.

Section 31(1)(a) sets out that information is exempt from disclosure if its release would or would be likely to prejudice the prevention or detection of crime.

To reveal the information regarding the number and nature of cyber-attacks would provide would-be or attempted attackers with information regarding our cyber-defence provision. It would indicate whether attempts have been detected and/or successful. This information could be used by motivated individuals in order to target the University, or to adapt behaviour in order to avoid detection.

Section 31(1)(a) is a qualified exemption. This means that the University of Leeds is required to consider whether the public interest in the information outweighs the public interest in maintaining the exemption.

There is clearly a very strong public interest in protecting public authorities from crime. To release information which increases the University's vulnerability to cyber-crime would jeopardise our ability to provide services to our students (current, former and potential), and would put at risk personal, financial and commercial sensitive information. We therefore consider that there is a very strong public interest in maintaining the exemption. Conversely, we do not consider there to be any particular public interest in the disclosure of this information. While it is important for students and the public to understand that the University takes the threat of cyber-crime seriously, and are taking appropriate measures to

tackle it, we do not consider that this interest would be furthered by the release of this information.

We therefore consider that the public interest is firmly in favour of withholding the information in this case.

We hope this information is helpful. If you have any questions about this email, however, please do not hesitate to contact us on foi@leeds.ac.uk

If you are unhappy with the service you have received in relation to your request and wish to make a complaint or request a review of our decision, you can request an Internal Review. Requests for Internal Review should be made in writing using the following contact information:

Post: Mr D Wardle
Deputy Secretary
The University of Leeds
Leeds
LS2 9JT

Email: foi@leeds.ac.uk

Requests for Internal Review should be submitted within 40 working days of receiving the University's response to your request. Further information about how the University manages Freedom of Information requests and about our complaints procedure is also available on our website (www.leeds.ac.uk).

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted the review/complaints procedure provided by the University. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Kind regards

Chloe Wilkins
Freedom of Information Officer

Secretariat
University of Leeds