FOI Request dated 25/03/2024

Request Reference: 3114

A copy of the university's current IT incident response framework or model, including any relevant documentation outlining the processes and procedures followed during critical incidents.

- *Details about the university's notification and escalation procedures within the incident response model.*
- *Information regarding the roles and responsibilities assigned to different teams or individuals during IT-related critical incidents, as outlined in the university's incident response model.*
- *Communication strategies employed by the university during critical incidents, including any predefined communication channels and messages specified in the incident response model.*
- *Information on how the incident response model seamlessly integrates with the university's existing IT infrastructure, with a focus on addressing incidents affecting critical systems or services.*
- *Policies and practices that facilitate collaboration between different departments and teams during critical incidents, as outlined in the incident response model.*

Response

We can confirm we hold information relevant to your request, however we are unable to provide the requested information on this occasion, in line with Section 17 of the Act, this response acts as a Refusal Notice. The Act contains a number of exemptions that allow public authorities to withhold certain information from release.

We have applied the following exemption to your request – **Section 31 (1)(a) – Law Enforcement.**

As with other large organisations; universities are reliant on the smooth running of their IT Networks. Maintaining the security of these networks is a significant challenge for all universities, who are increasingly subject to both general cyber security threats and targeted attempts to obtain information from students/staff. Release of any information under the Act represents a disclosure to the word, and it is our belief that if information was disclosed about the Universities comprehensive notification and escalation procedures, delineated roles and responsibilities, effective communication strategies, integration with existing IT infrastructure, and collaborative policies during critical incidents, a motivated individual or group could use this information to target any potential vulnerabilities, exposing the University's IT systems to various types of unlawful attack, and consequently prejudicing the prevention of criminal activity.

Having determined the aforementioned, in that disclosure of this information would expose the University to a real and significant risk of crime, application of S31 (1) Law Enforcement also requires us to consider the public interest in withholding/disclosing the information.

Factors in favour of disclosure –

• Increase public understanding of the University's information technology systems and processes, and how it manages its business.
• Enhancing the transparency and accountability of our cyber security system and about our ability to protect our systems and assets.

Factors against disclosure –
• Protecting the ability of public authorities to protect valuable public assets acquired with public funds.
• There is a strong public interest in not publishing information which might expose the University to cyber-attacks and in preventing criminal activity that could damage the running of the University and the security aspect of the information held.

After considering the above factors, we believe the factors against disclosure outweigh those in favour, and therefore apply Section 31 on this basis.