PRESS RELEASE

CSA CAUTIONS UNIVERSITIES TO ADHERE TO THE CII DIRECTIVE FOLLOWING THE UNIVERSITY OF NOTTINGHAM CYBER-ATTACK

Following a recent cyber-attack on the University of Nottingham in the United Kingdom, the Cyber Security Authority (CSA) is cautioning all Owners of Critical Information Infrastructure (CII), especially educational institutions, to adhere to the Directive for the protection of CII, launched in October 2021.

The University of Nottingham incident should serve as a reminder that no educational institution, regardless of its size, reputation, or technological sophistication, is immune to cyber threats. The incident is believed to have affected approximately 450,000 students and alumni, exposing sensitive information, including personal records, contact information, student identification details, and financial information.

While the breach may have occurred thousands of miles away from Ghana, its implications are relevant to our education sector and other CII sectors, such as Health, Telecommunications, and Transportation.

Ghana's universities are undergoing rapid digital transformation with student information systems, online learning environments, cloud services, digital payment platforms, and research collaborations becoming increasingly common. While these innovations improve efficiency and accessibility, they also expand the attack surface available to cybercriminals. The question is therefore not whether Ghanaian universities or other critical sectors will be attacked, but whether they are sufficiently prepared when an attack occurs.

The Directive for the Protection of CII

Recognising the growing threat landscape, the CSA has developed regulatory frameworks aimed at strengthening cybersecurity across critical sectors. The CII Directive seeks to ensure that operators of critical digital systems implement appropriate safeguards to protect essential services and national interests.

The Directive encourages organisations to establish cybersecurity governance structures, conduct risk assessments, implement security controls, report incidents, perform regular audits, and develop robust incident response capabilities to reduce the likelihood and impact of cyber-attacks.

Issued by the Cyber Security Authority
June 16, 2026

Ref: CSA/COMMS/PR/2026-06/01