June 14, 2024

BOT Agenda Item VIII.B.

UNIVERSITY OF
NORTHERN
COLORADO

MEMO

To: University of Northern Colorado Board of Trustees
From: Phillip Wyperd, CIO, Matthew Langford, CISO
Re: GLBA 2.0 Cybersecurity briefing
Date: May 3, 2024

In adherence to the Gramm-Leach-Bliley Act (GLBA) requirements, Information Management and Technology (IM&T) provides the University of Northern Colorado Board of Trustees with an annual cybersecurity report.

The GLBA became a law in 1999 and seeks to protect consumer financial privacy. GLBA was updated, and new requirements went into effect on June 9th, 2023. This requires additional controls to be met to ensure compliance with our financial audits. These compliance updates now require UNC to better track our 3rd party data partners, ensure cybersecurity training is required for our staff, and report to the Board of Trustees at least annually.

IM&T is confident in our cybersecurity posture and policies that protect UNC's financial data. Our recent financial audit with RubinBrown indicated no findings related to cyber data protection or policies. Eide Bailly's campus audit also found no findings related to UNC's cyber security posture and policies.

One of our top risks continues to be the compromise of sensitive data from external third-party companies possessing UNC data. As part of GLBA, IM&T is implementing a third-party partner tracking program that monitors outside companies that possess UNC data to comply with GLBA 2.0 requirements.

E-mail phishing campaigns are another concern. Attacks are becoming more sophisticated and user education is the best and most cost-effective way to address this risk. IM&T has invested significant resources to modernize our defense against phishing campaigns, but our partners must stay updated and informed. IM&T has started holding cyber security training events to share information with our partners. UNC must require cyber security training for all staff members.

IM&T dedicates significant time and resources to protecting the campus community from constantly involving cyber threats. Protecting our students, faculty, and staff from harmful cybersecurity events is paramount. Having the appropriate resources and support is crucial to our success. We would like to recognize and thank our campus leadership for funding resources and supporting IM&T's cybersecurity initiatives.