UNIVERSITY OF NORTHERN COLORADO

MEMO

To: University of Northern Colorado Board of Trustees
From: Phillip Wyperd, CIO, Matthew Langford, CISO
Re: Annual Cyber Security Report
Date: May 23, 2025

As part of the Gramm-Leach-Bliley Act (GLBA), Information Management & Technology (IM&T) is required to provide the Board of Trustees with an annual cybersecurity report.

IM&T is pleased to report that UNC had no significant cybersecurity incidents this year.

IM&T is confident in our cybersecurity posture and policies that protect UNC's financial data. Our state financial auditors had no findings related to UNC's cybersecurity. IM&T procured a security and network evaluation from an outside firm, and the only significant finding was that parts of our networking environment were close to being obsolete. Fortunately, the State of Colorado awarded $5.3 million of Joint Technology funding to UNC for modernizing our networking infrastructure.

To increase network security, IM&T partnered with multiple campus departments this year to improve the security of their systems. This necessary work meant time-consuming and complex network changes. IM&T would like to acknowledge our Athletics, Facilities, and UNC PD partners.

We continue to improve the integration of security intelligence systems with our threat response tools. This allows us to detect anomalies quickly and helps streamline threat mitigation when needed. We want to highlight the efforts of the IM&T security engineers who improve these systems weekly and constantly monitor for malicious activity outside of normal business hours.

The two most significant threats we face continue to be third-party data loss and phishing attacks. We regularly evaluate our partners for compliance to mitigate third-party data loss and implement new safeguards such as contractual security requirements, audits, and incident response protocols. We had no reported third-party data loss to the university this year. To control and contain credential loss from phishing attacks, we use multifactor authentication, deliver annual training to faculty and staff, and conduct regular internal phishing tests.

We monitor these risks closely and apply layered defenses to limit access, protect our systems, prevent exploitation, and do our best to stay ahead of threats. IM&T aims to maintain a resilient and responsive cyber-secure environment that protects our universities' students, personnel, data, operations, and reputation.