MEMO

To: University of Northern Colorado Board of Trustees
From: Phillip Wyperd, CIO, Matthew Langford, CISO
Re: Annual Cyber Security Report
Date: May 23, 2026

As part of the requirements of the Gramm-Leach-Bliley Act (GLBA), Information Management & Technology (IM&T) provides the Board of Trustees with an annual cybersecurity report. IM&T is pleased to report that the university's state financial auditors reported no cybersecurity-related findings, reflecting the strength of UNC's cybersecurity posture, policies, and practices for protecting institutional financial data.

IM&T also extends its appreciation to the State of Colorado's Joint Technology Committee for awarding UNC $5.3 million to modernize the university's networking infrastructure. This project is currently underway and is expected to be completed by July 1, 2027. The modernization effort will strengthen UNC's cybersecurity posture through the replacement of obsolete hardware and the implementation of an updated network architecture designed to improve resilience, reliability, and security.

The most significant cybersecurity threats facing the university continue to be third-party data loss and phishing attacks. During the year, UNC was one of many higher education institutions across the country impacted by the Instructure - Canvas data breach. While the investigation determined the incident did not involve passwords, financial information, or Social Security numbers, it did include FERPA data. This event reinforced the importance of strong vendor oversight, proactive monitoring, and layered cybersecurity protections across the university environment. To mitigate risks associated with third-party vendors and partners, UNC regularly evaluates compliance standards and implements safeguards such as contractual security requirements, audits, incident response protocols, multifactor authentication, and continuous security monitoring.

To reduce the risk of credential compromise from phishing attacks, the university enhanced multifactor authentication by disabling SMS verification and requiring end users to use a mobile based authentication application. Additionally, as part of an internal training program, IM&T conducted regular internal phishing assessments. We also want to recognize the dedication of the IM&T security team, whose ongoing efforts to enhance these systems and monitor for malicious activity — often outside of normal business hours — play a critical role in protecting the university environment.

IM&T remains committed to closely monitoring emerging threats and applying layered security defenses to protect university systems and data. Through continuous improvement, proactive monitoring, and responsive security practices, IM&T strives to maintain a resilient and secure technology environment that safeguards UNC's students, employees, operations, data, and institutional reputation.