UNC GREENSBORO
Board *of* Trustees

Compliance, Audit, Risk Management and Legal Affairs (CARL) Committee
November 10, 2026
10:45 a.m.

Discussion Item

CARL-3 Information Technology Services Update

Background Information

Donna Heath, Vice Chancellor for Information Technology Services, and Casey Forrest, Associate Vice Chancellor for Enterprise Infrastructure and Chief Technology Officer, will provide an update on information technology services projects.

Attachment

3.1 Information Technology Services Update

UNCG Information Technology Services

Compliance, Audit, Risk Management and Legal Affairs Committee

November 10, 2026

Donna Heath
Vice Chancellor for Information Technology Services
& Chief Information Officer

Casey Forrest
Associate Vice Chancellor for Enterprise Technology
Infrastructure & Chief Technology Officer

UNC GREENSBORO
Information Technology Services



Security Activity

UNCG perimeter defenses

BLOCKED BRUTE-FORCE ATTEMPTS

~1.23 million

Reported 30-day period*

Approximately 41,128 attempts per day

INBOUND PHISHING ATTEMPTS

90,922

September 26 to October 26, 2026

INBOUND MALWARE ATTEMPTS

1,365

September 26 to October 26, 2026

*Exact dates for the brute-force reporting period were not supplied.

Annual Security Awareness Training

October 2026 campaign | Status as of October 26, 2026

ASSIGNED

3,179

users assigned

Campaign was still active when reported.

COMPLETED

45%

1,434 users

IN PROGRESS

3.5%

110 users

COMPLETION AS OF OCTOBER 26

45%



Refresh status before presenting

STINGAR Honeypot Deployment

Shared Threat Intelligence for Network Gatekeeping and Automated Response

WHAT STINGAR ADDS

Duke-developed decoy services help defenders study hostile traffic and share near-real-time threat intelligence.

UNCG DEPLOYMENT

Externally Accessible Decoy Server

IP LIST TODAY

Not Used for Blocking

PLANNED INTEGRATION

Splunk + SOAR



INTERPRETATION

Decoy observations, not production breaches.

Automated perimeter blocking through Splunk and SOAR remains planned until deployed and validated.

STINGAR Observed Activity

Initial observations from the UNCG decoy environment

OBSERVED BEHAVIOR

Authentication attempts and malicious commands inside the decoy

FIRST OBSERVED ATTACK

Within 5 Minutes

FIRST 48 HOURS

More than 5,000 attacks

APPARENT SOURCE-IP LOCATIONS

United States, Kenya, Tunisia, Iran, and China

These IP locations do not establish actor identity or nationality.

These counts do not establish production breaches or the number of unique attackers.

AI Requests and Business Purposes

Portfolio scope and reported purposes in request descriptions

67 AI-related requests

Research and academic work	Literature discovery, coding, and transcription
Administration	Workflows, procurement, HR, and advancement
Teaching and student support	Engagement, simulation, advising, and accessibility
Communications and creative work	Websites, email, proofreading, and media production

Request records do not establish deployment, active use, or realized benefits.

AI Data Classification

Reported sensitivity across 67 AI-related requests

17 requests involve Confidential or Restricted data

Reported classification	Requests	Share
Level 1 Public	**25**	37.3%
Level 2 Internal	**25**	37.3%
Level 3 Confidential	**10**	14.9%
Level 4 Restricted	**7**	10.4%

Confidential and Restricted account for 25.4% of requests.

Percentages use all 67 records and round to one decimal place.

Planned Work Through December 2026

Security priorities and ongoing review work

CONTINUING

Privileged-Access Reviews

Oracle, Banner, database, and global administrator accounts.

NOVEMBER

Simulated Phishing Campaign

Campaign scheduled for November 2026.

PLANNED

Splunk Enterprise Security Premier

Risk-based analytics, correlation, and SOAR-enabled response.

Also continuing: AI security and governance reviews of platforms, agents, and data protection.

Questions?

UNC GREENSBORO
Information Technology Services