FAYETTEVILLE STATE UNIVERSITY™

Board of Trustees
Committee Meeting
Rudolph Jones Student Center
Room 242

COMMITTEE ON LEGAL, AUDIT, RISK AND COMPLIANCE

Wednesday, June 11, 2025
11:35 am

AGENDA

Call to Order	Glenn Adams, Committee Chair
Welcome and Opening Remarks	Glenn Adams
Roll Call	Karen Bussey
Approval of Minutes:	March 26, 2025

Information Items:

A. Data Privacy	Charlie Mewshaw *Chief Information Security & Privacy Officer*

Action Items:
There are no action items to be presented at this committee meeting.

Committee Members: Glenn Adams, Warren McDonald, John McFadyen, Frederick Nelson, Jerry Gregory, Kimberly Jeffries Leonard

Staff Liaison: Wanda Jenkins
Board Professional: Tamara Davis

For further information, please contact:
Wanda Jenkins
General Counsel and Vice Chancellor for Legal, Audit, Risk and Compliance
910.672.1145

Board of Trustees
Meeting Minutes
DRAFT

COMMITTEE ON LEGAL, AUDIT, RISK, AND COMPLIANCE

Wednesday, March 26, 2025

11:35 a.m.

The Committee on Legal, Audit, Risk, and Compliance (LARC) of the Fayetteville State University Board of Trustees convened Wednesday, March 26, 2025, in the Rudolph Jones Student Center, Multi-Purpose Room 242, and via Microsoft Teams. Committee Chair Glenn Adams called the meeting to order at 11:35 a.m.

ROLL CALL

The following trustees were in attendance in person: Mr. Glenn Adams, Mr. John McFadden, Mr. Frederick Nelson, Mr. Jerry Gregory, and Dr. Kimberly Jeffries Leonard.

APPROVAL OF MINUTES
It was moved by Trustee Frederick Nelson and seconded by Trustee John McFadyen that the December 11, 2024, and February 14, 2025, minutes be approved. The motion carried.

RISK, COMPLIANCE, AND EQUITY UPDATE
Assistant Vice Chancellor Beth Hunt presented the Top 2025 University Risks as part of the UNC System's Risk Register requirements under UNC Policy 1300.7. The policy requires each campus to annually collect, analyze and present to the UNC System Office the top 5 risk and that the board would need to vote on the top 5 risk. The Risk Register submission is due by June 15, 2025, to the System Office. AVC Hunt informed the committee that the risks are broken down by probability and urgency with five levels from rare to almost certain for risk probability and three levels for urgency, from long-term to immediate. The risk categories are Financial, Health & Safety, Operational, Reputational, Legal Regulatory & Compliance, and Strategic. The Risk impact has five categories, minor, moderate, substantial, critical, and catastrophic. AVC Hunt shared that Protection of Minors on Campus and New Construction that were items on the last risk impact report are no longer on the report.

The risks presented to the Committee include state and federal regulatory changes, deferred maintenance, campus safety including mental health, enrollment including funding adjustments, and cyber security. The trustees discussed the five risks, including the ranking. Trustee Glenn Adams asked for the UNC System's final compiled report be shared.

Action Item LARC-1: Top 5 University Risks
Trustee Frederick Nelson moved that the top 5 risks, as presented, be accepted by the Committee on LARC and recommended to the Full Board for approval. The motion was seconded by Trustee Jerry Gregory. The motion carried.

INTERNAL AUDITOR UPDATE
Mr. Jesse Chroman, Internal Auditor, presented an update on the procurement and purchasing card programs. The UNC System Office issued a new regulation on November 7, 2024, requiring internal auditors to assess compliance. Upon assessing compliance with the new regulation, Mr. Chroman concluded that as of January 29, 2025, the University was not in compliance with the regulation. However, the University has made progress towards alignment. Full compliance is anticipated prior to the next scheduled review. FSU's certification was submitted to the Systems Office on January 31, 2025. Mr. Chroman informed the committee that this will be an ongoing process. FSU will be recertified every January 31st. Trustee Glenn Adams commented on the timeframe of the new regulation's issuance and understanding that the university is in the process of implementing changes to be compliant.

Further, the UNC System Office issued a new regulation on February 26, 2025, requiring institutions to have policies and protocols in place that facilitate timely warnings and emergency notifications. The University is currently assessing compliance and testing.

Other activities include awaiting response of the Risk-Based Audit Plan Validation from the Office of State Budget and Management and an upcoming External Quality Assessment Report planned for Fall 2025.

ADJOURNMENT
The Committee on LARC adjourned at approximately 12:17 p.m.

Respectfully submitted,

Glenn Adams, Chair
Tonya Frederick, Recorder

FAYETTEVILLE STATE UNIVERSITY™

BOARD OF TRUSTEES COMMITTEE ON LEGAL, AUDIT, RISK AND COMPLIANCE

Wanda L. Jenkins

General Counsel and Vice Chancellor for Legal, Audit, Risk and Compliance

June 11, 2025

FAYETTEVILLE
STATE UNIVERSITY™

DATA PRIVACY PROGRAM

Charlie Mewshaw
Chief Information Security & Privacy Officer

CURRENT STATE OF PRIVACY LAW

Federal/National Privacy Regulation

GDPR

Cross-border data transfer safety and data privacy rights of citizens (EU)

CCPA/CPRA

Consumer rights and consent to personal data use (California)

PIPEDA

Privacy rights document for private sector organizations (Canada)

Industry Privacy Regulation

HIPAA

National standard for privacy governance of health-specific documentation

GLBA

Federal law for financial institutions pertaining to customer data privacy

FERPA

Enforces data privacy and consent of students and their parents

Information Security Privacy Frameworks

NIST Privacy Framework 1.0

Privacy framework mapped across five functional areas that encourages proactive privacy planning

ISO/IEC 27701

Operational controls mapped against GDPR articles for organization's specific compliance requirements

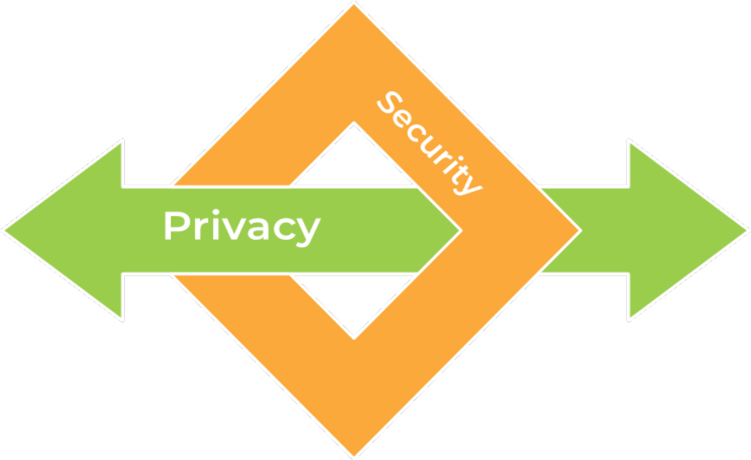
FAYETTEVILLE STATE UNIVERSITY

PRIVACY VS. SECURITY

Security *supports and facilitates* privacy but is not in itself a guarantee of compliance.

Privacy starts and ends with the focus on personal data**.**

- Beyond protection, privacy extends to understanding why personal data is being collected, what the lawful uses are, how long it can be retained, and who has access to it.



Security's role is to protect and secure assets, of which confidential data is a significant focus.

- The consequences of a personal data breach can be severe, including the loss of customer trust and potential regulatory consequences. We often think of how we use security to protect data.

FAYETTEVILLE
STATE UNIVERSITY™

UNC SYSTEM OFFICE POLICY 1300

Safeguarding sensitive information in alignment with UNC System Office Policy 1300 is a critical priority for Fayetteville State University.

FSU ITS is launching an Enterprise Data Privacy Program

- Program will ensure compliance with data protection regulations, maintain trust with stakeholders, and protect valuable assets.
- Program will be aligned with ISO 27701, the international standard for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).

UNC SYSTEM IT GOVERNANCE PROGRAM CHARTER

“In addition to addressing privacy as referenced in the most recent version of ISO 27002, each UNC institution will leverage its IT risk management approach in partnership with the institution's compliance function to determine the appropriate privacy policies to implement and the frequency of privacy risk assessments.”

Formalizing a Privacy Information Management System (PIMS) will:

- align FSU with UNC System Office requirements for data privacy
- leverage the ISO 27701
- implement the complementary Information Security Program, ISO 27002.

PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS)

- As part of developing a PIMS, the University must identify and include interested parties in communications and operations related to the program.

- This program will outline our approach to data privacy governance, risk management, data handling practices, and continuous monitoring. It will enable us to systematically address privacy concerns while ensuring that we remain accountable to stakeholders, customers, and regulators alike.

- Stakeholders have been identified to support and engage with this initiative as to uphold the highest standards of data privacy and compliance.

PHASED APPROACH BENEFITS

IT Benefits

☑ Identification of information security-specific privacy controls, mapped against governing privacy frameworks (GDPR, CCPA, FERPA, PIPEDA, NIST, ISO).

☑ Comprehensive inventory of where personal data exists within IT systems at different points during its lifecycle (at rest, in transit).

☑ Perspective from a privacy lens on IT controls (system and network access, asset management, etc.).

☑ Assigned ownership for members of the IT team of privacy-IT integration and individual privacy initiatives.

FSU Benefits

Understanding of the scope if privacy within the context of the organization.

An active role and participation in the integration of privacy requirements as a part of pre-existing operations, as well as net-new operating procedures.

Ability to leverage privacy as a competitive advantage in streamlining how customer data flows through the organization.

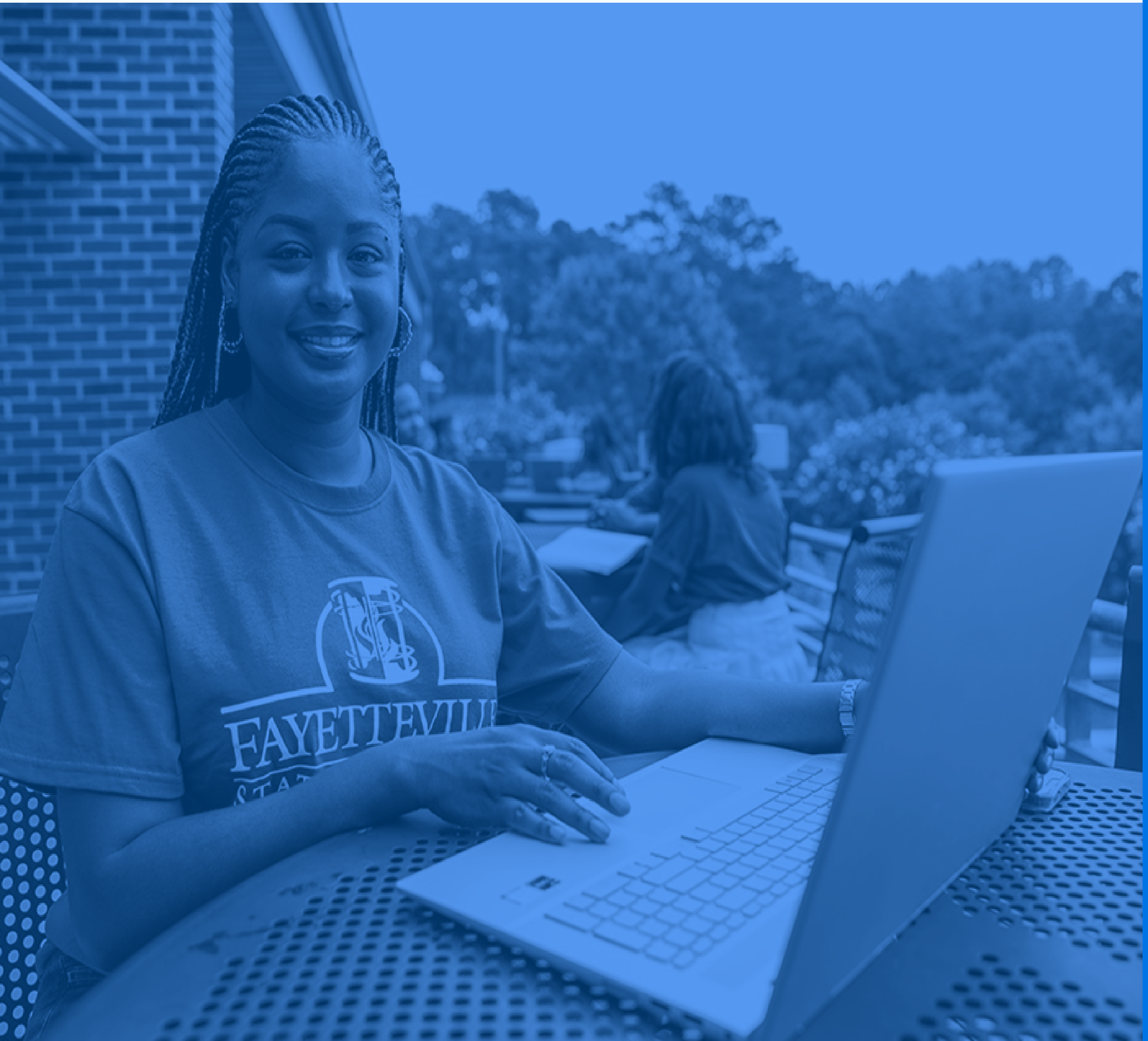
Thorough perspective on how each of the business units’ processes impact and reference personal data.

OVERARCHING INSIGHT

FSU aims to strengthen our commitment to protecting University and personal data, enhancing transparency, and minimizing privacy risks across all University operations.

- **Quantitative Approach**: Using metrics and a risk-based approach to drive a privacy program that supports compliance and considers the custom needs of Fayetteville State.
- **Iterative Process**: Prioritizing privacy initiatives based on value and risk and support the rollout through customized metrics that suit Fayetteville State.
- **Compliance**: Ensuring compliance with evolving state, national, and global privacy regulations and foster a culture of privacy awareness throughout our campus

PROTECTING PERSONAL DATA



FSU will focus on all personal data, whether it’s publicly available or private.

- Building the privacy program includes:
  - defining how the data is processed
  - creating notices and capturing consent, and
  - protecting the data itself.
- An effective privacy program also enables accessibility to information based on regulatory guidance and appropriate measures.

PHASED APPROACH

	1. Collect Privacy Requirements	2. Conduct a Privacy Gap Analysis	3. Build the Privacy Roadmap	4. Implement and Operationalize
Phase Action Items	1. Define and document drivers 2. Establish privacy governance structure 3. Build a privacy RACI chart 4. Define personal data scope 5. Build a risk map	1. Complete a *Data Process Mapping Tool* 2. Compare compliance and regulatory requirements with gap analysis 3. Assess and categorize privacy gap initiatives	1. Finalize privacy gap initiatives 2. Prioritize initiatives based on **cost, effort, risk,** and **business value** 3. Set firm dates for launch and execution of privacy initiatives 4. Assign ownership for initiatives	1. Establish a set of metrics for the Data Privacy Program 2. Operationalize metrics 3. Set checkpoints to drive continuous improvement
Phase Outcomes	• Documented business and IT drivers for the privacy program • High-level understanding of how privacy is perceived in the organization • Completed *Data Privacy Program RACI Chart*	• *Data Process Mapping Tool* detailing all business processes that involve personal data • Privacy maturity ranking *(Privacy Framework Tool)* • Identification of compliance or regulatory privacy gaps	• Completed *Privacy Framework Tool* • Completed privacy roadmap, including timeline for initiative implementation, and cost/benefit vs. value/risk assessment	• Customized set of privacy metrics • Tasks to operationalize privacy metrics • *Data Privacy Report* document • Performance monitoring scheduled checkpoints

PHASE ONE: COLLECT PRIVACY REQUIREMENTS

Phase Action Items

1. Define and document drivers
2. Establish privacy governance structure
3. Build a privacy RACI chart
4. Define personal data scope
5. Build a risk map (meetings 2-3)

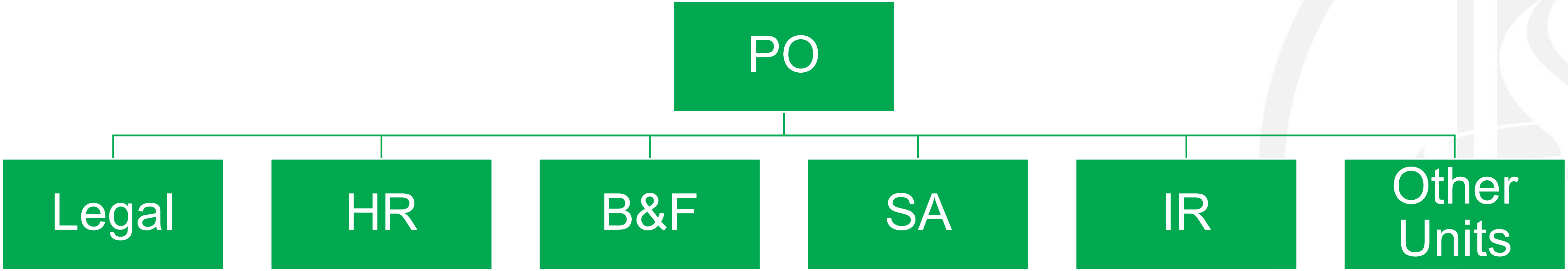
Phase Outcomes

- Documented business and IT drivers for the privacy program
- High-level understanding of how privacy is perceived in the organization
- Completed Data Privacy Program RACI Chart

CENTRALIZED MODEL

Fayetteville State University is creating an initial **centralized** organizational structure for managing privacy. In this case, a dedicated privacy team directs all the other departments in terms of their personal data management.

The centralized model is a traditional structure for privacy in the organization, and it promotes the idea that one group is entirely accountable for the proliferation of privacy within the organization, with responsibilities being stripped across other units. This structure requires regular reporting and communication between the different groups.


PO

Legal

HR

B&F

SA

IR

Other Units

QUESTIONS