FAMU FLORIDA A&M UNIVERSITY
PRIVACY PROGRAM
OFFICE OF COMPLIANCE AND ETHICS

Compliance Review

Date of Review: June 3, 2025

Review conducted by: La'Tonya Baker, Director of Compliance/Chief Privacy Officer

Approved by: Rica Calhoun, Chief Compliance and Ethics Officer

Process or procedure to be reviewed:
REASON: ☐New Regulation ☐Routine Review ☒Management Alert ☐Random Review

☐Other: ____

Scope of Review:

This review is intended for all members of the University who handle, transmit, or share data. It applies to all departments and employees who manage confidential information in the course of their University responsibilities.

Applicable Standards and Policies:

- FAMU Privacy Statement
- Information Technology Services (ITS) Security Guidance
- Student Handbook: Acceptable Use of Technology
- Florida Information Protection Act (FIPA) of 2014 – A state law requiring entities, including public universities, to implement safeguards for personal data and provide notification in the event of a breach.
- NIST 800-53 Control Family: Access Control (AC), System and Communications Protection (SC) – While not mandatory, these federal standards represent nationally recognized best practices and serve as a benchmark for strengthening institutional data security.

Summary:

This compliance review serves as a proactive reminder to the University community of the shared responsibility we all have in protecting the privacy and confidentiality of sensitive information. As the digital landscape evolves, so must our practices for handling institutional data. Email remains a convenient tool, but when used to transmit confidential information without safeguards, it can lead to avoidable risks and vulnerabilities. While there is no evidence of widespread misuse, we are taking this opportunity to reinforce best practices that mitigate the possibility of unintentional data breaches. This review highlights cloud-based file storage platforms (cloud-based applications) like Dropbox with Two-Factor Authentication (2FA), SharePoint and OneDrive as secure and efficient methods for sharing sensitive information, aligning with the University's privacy and compliance standards.

Key Issues and Risks Identified:

- Email remains a common method of communication, which increases the risk of accidental disclosure when sending attachments with sensitive information.
- Traditional email lacks advanced access controls and auditability.
- Inconsistent awareness or use of secure alternatives such as cloud-based applications.

Recommendations:

1) Promote cloud-based applications as a Standard for Secure File Sharing:
    a) Recommendation:
        i) Promote Dropbox with Two-Factor Authentication should be used when transmitting:
            (1) Student academic or conduct records
            (2) HR-related evaluations or personnel actions
            (3) Investigative files or disciplinary documentation
            (4) Financial, budgetary, or contractual information
            (5) Any Personally Identifiable Information (PII)
2) Cloud-based applications best practices:
    a) Enable 2FA on all accounts
    b) Use link sharing with expiration dates and view-only access
    c) Review and revoke access when no longer needed
    d) Avoid sending attachments via email when cloud-based applications can be used

3) Common Use Case Examples:

   a) Academic advisors sharing GPA or conduct files with department chairs

   b) Investigative offices sharing final reports and/or compliance reviews

   c) HR transmitting performance evaluations or documentation

   d) Procurement offices sending confidential vendor agreements

   e) Research departments transmitting grant budgets with collaborator institutions

4) Suggested Next Steps for Units:

   a) Departments and managers should assess current file-sharing practices and identify opportunities to adopt more secure alternatives

   b) Encourage departmental discussions on secure communication norms

   c) Collaborate with ITS or the Office of Compliance and Ethics Privacy Program for questions about approved tools and access controls

Conclusion:

Aligned with industry best practices, state law, and national standards, it is strongly recommended that departments and employees use cloud-based applications with 2FA for sharing sensitive information. This approach helps reduce the potential for unintentional breaches and aligns with our collective responsibility to safeguard University data.
By reinforcing these practices, we continue building a culture of privacy and accountability across campus.