Appendix A: Platform Security Chart

PLATFORM SECURITY CHART

UM DATA CLASSIFICATION	UM IT Managed Technology in UM Data Center [1]	UM Technology Connected to the Campus Network [2]	UM Box [3]	UM Office 365 and OneDrive [3]	UM Go Email and Drive [3]	Other UM Managed Cloud Services [3]	UM Mobile Technology [4]	Approved Dept. Software Applications [5]	Personally Owned / Managed Technology [6]
Instructional Data	✓	✓	✓	✓	✓	✓	✓	✓	✓
Student Educational Records (FERPA) [7]	!	!	✓	🔒	🔒	✗	🔒	✓	🔒
Protected Health Information (ePHI) [8]	!	!	!	✗	✗	✗	!	!	✗
Payment Card Industry Information (PCI)	✗	!	✗	✗	✗	✗	!	!	✗
Mississippi Data Breach Notification Law [9]	!	!	!	✗	✗	✗	!	!	✗
Other Sensitive Data [10]	!	!	!	✗	✗	✗	!	!	✗
All Other Non-Sensitive Data	✓	✓	✓	✓	✓	✓	✓	✓	✓

Platform Security Chart: References

1. Refers to systems such as SAP, Blackboard, etc. that are managed by professional IT staff with the highest security levels.
2. Refers to non-mobile, university-issued computers and storage devices connected to the campus network, which are outside of the University of Mississippi (UM) Data Center, or within the Data Center but not behind most restrictive Data Center firewalls.
3. UM IT implementations of Box, Google Apps, and Microsoft 365 offer a certain level of protection, but each user is responsible for managing their own shared access settings and preventing data exposure. Review account security and sharing settings often.
4. This includes university-issued computers and storage devices. The user is responsible for securing the device and preventing data exposure. Mobile devices approved to store sensitive data must be encrypted.
5. The department head is responsible for ensuring that the data and application is properly secured. Sensitive data must be encrypted.
6. Policy restrictions apply to storing UM data on a personal device, or storing it remotely using a personal account on a cloud service. This includes platforms such as Dropbox, iCloud, Adobe, AWS, and other hosting/storage/collaboration/messaging services.
7. Relevant email communication specific to an individual student is permitted. However, this communication is only permitted between official UM email platforms (@olemiss.edu and @go.olemiss.edu). Sets of data, which have not been de-identified, including grades and other non-directory information, may not be emailed. UM Registrar policies related to FERPA also apply.
8. The storage, processing, or transmission of any electronic Protected Health Information (ePHI) must be approved by the IT Security Coordinator. HIPAA affected areas may require additional resources including 3rd party audits at the expense of the department.
9. Mississippi law requires notifying individuals when particular personal information is digitally exposed. This includes an individual's first name, or first initial and last name, in combination with any of these elements: • Social Security number • State ID card number • Driver's license number • Financial/debit/credit account number with security password/code. Encrypted data is excluded.
10. Includes sensitive Identifiable Human Subject Research data, which requires UM Institutional Review Board (IRB) approval, in addition to approval by the IT Security Coordinator. Also includes Export Controlled Research data (ITAR, EAR), Gramm Leach Bliley Act (GLBA) financial data, and other federally designated Controlled Unclassified Information (CUI). Additional compliance needs and restrictions may be applicable. These resources are to be provided by the affected department.

Additional Notes on Sensitive Data

- Email is NOT a permitted medium for any un-encrypted sensitive data, unless specific exclusions are defined herein.
- All UM systems (servers, desktops, laptops, other mobile devices, etc.) with sensitive data MUST be in the UM System Registry

✓	▪ Permitted ▪ Must be protected as defined by UM policy
✗	▪ Not permitted
!	▪ Requires prior approval by IT Security Coordinator
🔒	▪ Do not email FERPA records to non-olemiss.edu addresses ▪ Devices (computers, tablets, phones, etc.) must adhere to specific security standards as defined by UM policy