ADMINISTRATIVE POLICY TEMPLATE

Policy Title	Bring Your Own Device (BYOD)
Policy Subtitle/Subject	Click or tap here to enter text.
Responsible Executive(s) (RE)	**Sr. VP and COO, Patrick Norton**
Responsible Office(s) (RO)	**Information Technology**
Primary Point of Contact from RO	**Chief Information Security Officer**
Contact Information	**ciso@tulane.edu**
Date Proposed	Click or tap to enter a date.
Reviewed	Click or tap to enter a date.
Last Updated	Click or tap to enter a date.
Effective Date	Click or tap to enter a date.

☒Permanent ☐Temporary

1.0 POLICY STATEMENT

Personally owned end-user devices are increasingly being used to connect to and access Tulane University information systems and data. This policy outlines the requirements for Tulane Users who use their personally owned end-user devices to access University information systems and data.

2.0 PURPOSE AND SCOPE

All members of Tulane University have a responsibility to protect University information systems and data from unauthorized access or disclosure. This responsibility extends to the use of personally owned devices to access University information systems and data. This policy establishes the key principles and minimum security requirements for personally owned end-user devices connecting to or accessing University information systems and data. This policy does not apply to Tulane-owned devices.

3.0 APPLICABILITY OF THIS POLICY

This policy applies to faculty, staff, students, contractors, consultants, affiliates, and all others granted access to Tulane information systems and data and who use personally owned end-user devices to access Tulane information systems and data.

4.0 WEBSITE ADDRESS FOR THIS POLICY

Enterprise Risk Services will add the web address of the policy after it is added to the policy library.

5.0 CONTACTS

Identifies persons or departments that should be contacted if there are any questions or concerns regarding the policy.

Subject	Contact	Telephone	E-mail/Web Address
Questions or clarifications regarding this policy	Chief Information Security Officer	504-988-8500	security@tulane.edu
Report an actual or suspected security incident	IT Service Desk	504-988-8888	help@tulane.edu

6.0 CONTENT

The table of contents identifies the pages to find relevant information in the policy.

7.0 DEFINITIONS

The terms "Tulane University", "Tulane", and "University" are used interchangeably and do not represent different areas, responsible parties, or systems.

End-User Device: An end-user device is any type of personal computer, consumer mobile device, or removable storage media that can access or store information. End-user devices must not act as servers or provide Internet-accessible services to others. End-user devices may be owned by Tulane University or by users personally. End-user devices include, but are not limited to:

- Desktop, laptop, and tablet computers
- Smartphones and other mobile/cellular phones
- Personal digital assistants
- Portable media devices (e.g., devices capable of playing digital media)
- Removable media (e.g., USB flash drive, memory card, external hard drive, writeable CD or DVD)
- Wearable computing devices (e.g., smartwatches)
- Any other device capable of connecting to a University network or otherwise accessing or

storing University data

Information Systems: Information systems are any and all computer or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of data. In addition, Tulane information systems are any technology or services that are owned or managed by Tulane University, that connect to the Tulane network, connect to another Tulane technology or service, or store Tulane data or information.

University Data: University Data is any data or information, regardless of electronic or printed form or location, that is created, acquired, processed, transmitted, or stored by the University. Where appropriate, University Data may be further defined as Administrative, Academic, or Research Data to provide additional management or information security guidance.

University Information Technology (IT): The central Information Technology department of Tulane University is responsible for networks, infrastructure, enterprise applications, and cybersecurity standards for the University. The University IT department provides a finite level of services to all departments/schools within Tulane University.

Users: Persons affiliated with Tulane University, including students, faculty, staff, affiliates, vendors, third-party consultants, etc. who utilize Tulane information systems or data.

8.0 POLICY AND PROCEDURES

It is the policy of Tulane University that all individuals using personally owned end-user devices to connect to Tulane information systems or access University data acknowledge and abide by the following requirements.

Tulane University reserves the right, through policy enforcement or technical means, to limit users' ability to transfer data to and from specific information systems. The University further reserves the right to restrict the use of or permanently disconnect any personally owned end-user device from Tulane information systems if that device disrupts or interferes with Tulane information systems or behaves in such a way that the services or security of University information systems or data are threatened.

8.1 Data Ownership.

All Tulane University data, regardless of its location, is owned by the University. Any data created on, transmitted to, received or printed from, or stored or recorded on an end-user device during the course of a user's affiliation with the University or on Tulane's behalf is the property of Tulane University, regardless of who owns the device. All Tulane University owned data must adhere to relevant policies and data protection requirements as detailed in Section 8.5 and Appendix I.

8.2 Data Preservation.

In some cases, such as to comply with applicable federal and state laws, regulations, policies, University contracts, and to gather information related to investigations or pending or potential litigation, Tulane may require a user to turn over or provide appropriate access to University data stored on a user's personally owned device. In such instances, and for Tulane to carry out its legal obligations, authorized personnel may access the entirety of the user's personally owned end-user device, search it using specialized software configured with appropriately tailored criteria, review the

information found by the search, and disclose relevant portions to University officials who are duly authorized to receive it. The University is not responsible for the loss of any personal data on a personally owned end-user device in such situations.

8.3 Device Monitoring.
University IT provides, manages, monitors, and maintains Tulane information systems and access to University data. Any personally owned end-user devices that connect to Tulane information systems or access University data may similarly be monitored, and the activities of such devices may be contained in University information systems logs. End users connecting personally owned end-user devices to Tulane information systems or accessing University data specifically acknowledge and consent to such monitoring.

8.4 Remote Wipe.
All mobile devices used to connect to Tulane information systems or access University data must have the ability to be remotely wiped in case of loss, theft, or if Tulane detects a data breach and potential exfiltration of University data. Tulane reserves the right to remotely wipe the device when necessary to protect Tulane information systems or data.

8.4.1 Protection of Personal Data
Users wishing to not have personal data wiped in the case of a remote wipe are required to follow the standards in Appendix 1: Tulane Device Standards. Use of these software applications will ensure only Tulane data is removed in the case of remote wipe. Accessing Tulane data outside of the identified applications place your personal data at risk for remote wipe.

8.5 Data Protection.
Follow all applicable laws and regulations, contractual agreements, and University policies, standards, and guidelines regarding the use and protection of Tulane information systems and data, including the University's Data Management Policy, Data Classification Policy, and any restrictions stated therein.

8.6 Minimum Security Requirements.
Follow the security protections outlined Appendix 1: Tulane Device Standards for the use of any personally owned end-user device that connects to any Tulane information system or accesses University data.

8.7 Reporting.
Immediately report any lost or stolen personally owned end-user devices that contain University data to the IT Service Desk (help@tulane.edu) and Tulane University Police Department.

9.0 CONSEQUENCE OF VIOLATING THE POLICY

Violation of this policy may result in disciplinary action, up to and including termination and/or criminal prosecution.

Failure to comply with the standards outlined here and in related policies may result in harm to individuals, organizations, or the University. Violations of this policy or any law related to the use of a Tulane information system, including, but not limited to the Family Educational Rights and Privacy Act

of 1974 (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Gramm-Leach-Bliley Act (GLBA), may result in penalties and disciplinary action under rules established by Tulane University.

APPENDIX I

Other Relevant Information or Policies

1. *Tulane Data Classification Policy*

2. *Tulane Data Governance Policy*

3. *Tulane Data Management Policy*

4. *Retention of Research Data Policy*

5. *Tulane Device Standards*

6. *Tulane Cell Phone Policy (draft – link to be provided)*

7. *Tulane Clinical Data and Information Policy (draft – link to be provided)*

8. *Tulane Policy Library*