ADMINISTRATIVE POLICY

Policy Title	Workstation and Mobile Device
Policy Subtitle/Subject	Workstation and Mobile Device
Responsible Executive(s) (RE)	**Chief Information Officer** **Chief Information Security Officer**
Responsible Office(s) (RO)	**Information Technology**
Primary Point of Contact from RO	**Chief Information Security Officer**
Contact Information (email and phone)	**ciso@tulane.edu ; 504-988-8500**
Date Proposed	**4/2/24**
Reviewed	**4/2/24**
Last Updated	**4/2/24**
Effective Date	**4/2/24**

☒Permanent ☐Temporary

1.0 POLICY STATEMENT

Tulane University's Workstation and Mobile Device policy outlines the guidelines and requirements for University technology resources used to access Tulane University information systems to perform work-related activities.

The Workstation and Mobile Device Policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

- Laptop/notebook/ultrabook computers
- Workstations
- Smartphones
- Other mobile/cellular phones
- Tablets
- Portable media devices

- Wearable computing devices
- Any other device capable of storing university data and connecting to a network

2.0 PURPOSE AND SCOPE

All members of Tulane University have a responsibility to protect University Information Systems from unauthorized access or disclosure. The purpose of this policy is to ensure the confidentiality, integrity, and availability of Tulane Information Systems being accessed by University technology resources. This policy will define the requirements for all University technology resources and the methods used to ensure the protection of University information systems in the event of a lost or stolen device, as well as other situations where access to Tulane Information Systems is no longer authorized. Tulane University shall implement safeguards to restrict access to authorized users for all devices with access to University data.

3.0 APPLICABILITY OF THIS POLICY

This policy applies to all Tulane users who use University technology resources to access, store, or transmit Tulane University information systems to perform work-related tasks.

The Tulane Bring Your Own Device (BYOD) policy covers requirements personally owned devices. A link to the BYOD policy can be found in ***Appendix 1: Related Policies, Laws, Regulations, and Processes.***

4.0 WEBSITE ADDRESS FOR THIS POLICY

www.policy.tulane.edu

5.0 CONTACTS

Subject	Contact	Telephone	E-mail/Web Address
Workstation and Mobile Device	Jeremy Pelegrin	(504) 988-8500	ciso@tulane.edu

6.0 CONTENT

1.0 POLICY STATEMENT 1
2.0 PURPOSE AND SCOPE 2
3.0 APPLICABILITY OF THIS POLICY 2
4.0 WEBSITE ADDRESS FOR THIS POLICY 2
5.0 CONTACTS 2
6.0 CONTENT 2
7.0 DEFINITIONS 3
8.0 POLICY AND PROCEDURES 4
8.1 Asset Management 4
8.2 Configuration Controls 4
8.2.1 User Responsibilities 5
8.3 Security Controls 5

8.4 Incidents Involving University Technology Resources 5

8.4.1 Remote Wipe 5

8.4.2 Lost or Stolen Devices 5

8.4.3 Security Incidents.....6

9.0 CONSEQUENCE OF VIOLATING THE POLICY 6

APPENDIX I 7

APPENDIX II.....7

7.0 DEFINITIONS

Bring Your Own Device (BYOD): A device that is personally owned by an individual.

Encryption: The process of protecting information or data by using mathematical models to scramble it in such a way that only the parties who have the key to unscramble it can access it. This process is managed via the operating system of the device and does not typically require additional software.

End of Life (EOL): When software or hardware is no longer supported or deemed unable to provide functionality or compliance with organizational security or regulatory requirements.

Information Systems: Information Systems are all computer or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of data.

Jailbreak: To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. Jailbreaking gives access to the operating system, thereby unlocking all its features and enabling unauthorized software installation. This process is also referred to as "rooting" or "root".

MFA: Multi-Factor Authentication. Multi-factor authentication is an electronic authentication method in which a user is granted access to a system only after successfully presenting two or more pieces of information to verify a user's identity to an authentication mechanism.

Operating System (OS): The software which runs the interface of a computer. (Windows, iOS, Linux)

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

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, 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.

University Technology Resources are any technology devices or services that are owned or managed by the University, that connect to the University network, connect to another University technology or service, or store University data or information.

Virtual Private Network (VPN): A service that establishes a digital connection between a computer and a remote location, creating a point-to-point tunnel that encrypts data transmission and provides a secure connection.

8.0 POLICY AND PROCEDURES

8.1 Asset Management

Each department shall ensure that devices adhere to the following restrictions:

1. The device does not exceed 8 years of age, or
2. The warranty period is not exceeded by 3 years.

Devices which are outside of these restrictions must be replaced. Devices older than 8 years will not be allowed to connect to Tulane information systems.

University technology resources not in use must be returned to Property Management. Additional information can be found at https://pm.tulane.edu/

Any transfer of equipment associated with sponsored projects shall adhere to the Tulane University Guidelines for Transferring Equipment Associated with Sponsored Projects. Additional information can be found at https://tulane.box.com/s/frd9r5i5vkytsvvhdlwkt25jnlgkg7zc.

In the event of evacuation or decommission of a location, university technology resources shall be gathered for use at the alternate site. Check with your department IT representative or manager to determine your responsibilities in this process.

8.2 Configuration Controls

To protect the Tulane information system being accessed, the following configuration controls below must be adhered to for all University technology resources.

1) Enrollment or management through a university approved Mobile Device Management (MDM) or configuration management system.
2) Enable disk encryption for all devices accessing University information systems.
3) Have University provided anti-malware software always installed and active.
4) Regularly install security patches and other updates to application software.
5) Devices shall be updated regularly with the latest vendor software updates and University IT approved OS. No end-of-life operating systems will be allowed to access Tulane information systems.
6) Employ access protection using a passcode, passphrase, fingerprint, or other electronic means.
7) Comply with all policies, laws, regulations, or processes applicable to the Tulane resource being accessed. Please contact the Responsible Office within the applicable policies as found in Appendix I for any questions.
8) Devices shall NOT be Jailbroken or otherwise altered to change built-in protections.

Exceptions to any of the above configuration controls must be approved by University IT.

8.2.1 User Responsibilities

a) Users should not store any personal data, including email, on their university technology resource. This data will not be considered in the event of a failure, loss, or recovery of a device.

b) Applications shall only be installed from official platform-approved sources (device stores). Installation of applications from untrusted sources is forbidden.

c) Non-enterprise applications are the responsibility of the purchaser. Responsibilities include appropriate license management, updates, and compliance with the regulatory requirements associated with the university information system.

8.3 Security Controls

The following security controls shall be enforced:

1) Only University technology resources managed by IT, department/school IT, or authorized by IT shall be allowed to connect to the back-end (i.e. databases, development systems, programming code, Enterprise System source code) of Tulane information systems.
2) Access to ports (ie. USB, external media) on university technology resources may be restricted for compliance purposes where necessary (ie. HIPAA).
3) Any attempt to bypass the MDM implementation will result in immediate disconnection from all University information systems.
4) Any device which represents a potential threat to University information systems will be prohibited from connecting to all University networks and information systems.
5) Sensitive data such as personal information will not be stored on University technology resources without approval by Tulane University IT.
6) Users shall not load pirated software or illegal content onto university technology resources.

8.4 Incidents Involving University Technology Resources

8.4.1 Remote Wipe

By connecting to Tulane University technology resources, devices gain the capability of being wiped remotely by University IT.

When the user or the IT department initiates a remote wipe, the device will be wiped of all data and settings. Wiping data, documents, files, settings, and applications in the event a device is lost, stolen, or compromised in any way is critical to protecting University data.

8.4.2 Lost or Stolen Devices

Tulane users must report lost or stolen university technology resources immediately to the Information Technology department and comply with Tulane University's incident response procedures – *pending link upon 2024 revision*

Remote wipe capabilities may be activated on lost or stolen devices to protect University Data.

8.4.3 Security Incidents

Tulane users must report any suspected security incidents, data breaches, or unauthorized access involving university technology resources immediately to the Information Technology department and comply with Tulane University's incident response procedures.

8.4.4 Litigation or Other Investigations

In the event of litigation or other investigations, the Tulane user will be required to cooperate fully in ensuring the obligations of the University are met. This could include an investigation of the university technology resource following the guidelines of the applicable policies as found in Appendix I.

8.5 Other Security Controls

Tulane users are responsible for ensuring that they adhere to all applicable security controls relevant to the Tulane information system being accessed by their university technology resource.

These include, though are not limited to:

1) Research and Data Retention Policy
2) PCI Policy – *currently in draft form*

Links to these and other policies can be found in ***Appendix 1: Related Policies, Laws, Regulations, and Processes.***

8.6 Termination or Separation

Upon termination or separation any university technology resource must be returned to University IT or the department IT representative. Failure to comply may result in the use of remote wipe capabilities.

In the event of an internal transfer to a new department within the University, any university technology resource must be returned to University IT or the department IT representative. Failure to comply may result in the use of remote wipe capabilities.

9.0 CONSEQUENCE OF VIOLATING THE POLICY

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

Failure to comply with the standards outlined here and in related policies may result in harm to individuals, organizations, and/or the University. Violations of this policy or any laws related may result in penalties and disciplinary action under rules established by the University.

APPENDIX I

Related Policies, Laws, Regulations or Processes

Bring Your Own Device (BYOD) Policy – *currently in draft form*

Data Management Policy - https://tulane.box.com/s/brp4hwga1i7h13wwsgoc0j3xd96y0w7e

Data Classification Policy - https://tulane.box.com/s/ue4asoz6futr782qbliu72ojef51f2q8

Governance and Retention of Research Data –
https://tulane.app.box.com/s/b6pjarrmspfu2x8wl68wkymi7hcinbfq

Tulane IT Policy Library - https://it.tulane.edu/policies-guidelines-and-recommendations

Tulane Policy Library - https://policy.tulane.edu/policy-library

Tulane PCI Policy – *currently in draft form*

APPENDIX II

Include an approved vendor's list – link to Procurement location