ADMINISTRATIVE POLICY

Policy Title	Physical Access Management
Policy Subtitle/Subject	Physical Access Management
Responsible Executive(s) (RE)	**Sr. VP and COO, Patrick Norton**
Responsible Office(s) (RO)	**Campus Services**
Primary Point of Contact from RO	**Kirk Bouyelas Associate Vice President Public Safety and Community Engagement**
Contact Information (email and phone)	**504-257-1352**
Date Proposed	**5/17/23**
Reviewed	**5/17/23**
Last Updated	**5/17/23**
Effective Date	**5/17/23**

☒Permanent ☐Temporary

1.0 POLICY STATEMENT

To protect the individuals, property, and privacy of the Tulane University campus and community, the University limits access to facilities, buildings, and spaces. Campus Services will maintain appropriate procedures and controls and will work with other departments to ensure facilities maintain both accessibility and security.

2.0 PURPOSE AND SCOPE

The purpose of the Physical Access Management Policy is to regulate physical access to Tulane University facilities, buildings, and spaces. This policy will provide individuals with awareness of their responsibilities when granted physical access within Tulane University.

3.0 APPLICABILITY OF THIS POLICY

This policy is applicable to all faculty, staff, students, vendors, contractors, consultants, visiting scholars and researchers, and others, who require physical access to Tulane University facilities, buildings, and spaces.

4.0 WEBSITE ADDRESS FOR THIS POLICY

https://policy.tulane.edu/policy-library

5.0 CONTACTS

Subject	Contact	Telephone	E-mail/Web Address
Physical Access	Kirk Bouyelas	(504) 247-1352	

6.0 CONTENT

7.0 DEFINITIONS

Access Device/s: Any means or device used to lock, unlock, open, or gain access into a

secured area. This includes but is not limited to metal key, combination, keypad code/personal identification number, access card, biometric, mobile device credential, RFID (radio frequency identification), or combination thereof.

Access Device Holder: Persons granted physical access to Tulane facilities. Access device holders are responsible for maintaining building security by keeping access doors closed and locked. An access device holder is responsible for all access devices issued to them and must return all issues access devices to the issuing department upon separation.

Administrator: for the purpose of this policy, an administrator is the President and Sr. Vice Presidents. Vice Presidents, Associate Vice Presidents and Assistant Vice Presidents of departments essential to providing services related to emergency response, security, operations, risk management and facilities management are also considered administrators under this policy.

All-Access: All-access is an access device which opens every one of a given set of locks or grants access to buildings through exterior doors.

Authorized Personnel: Faculty, staff, students, vendors, contractors, consultants, visiting scholars and researchers, and others, who are approved to receive or maintain physical access within Tulane University.

Campus Services: Group who will be the primary administrator of the physical access control program and shall work in coordination with Information Technology to implement the access control program and perform annual access control audits. This group shall ensure compliance with the authorization requirements for access levels (Appendix 1).

Department Heads: University employees with overall responsibility for a building, space or group of spaces. This may include Vice Presidents, Deans, Associate Vice Presidents, or Assistant Vice Presidents. Department heads are responsible for assigning a Department Access Coordinator (DAC), approval of all access requests to facilities under their control, verifying that all issued access devices are returned, and access is terminated for anyone that is separated from the University or no longer requires access to the facility, verifying that all building access holders are reported to Campus Services annually, and ensuring compliance with this policy.

Department Access Coordinator (DAC): A person designated by a Department Head, to be responsible for processing access control requests for the department. Responsibilities of the DAC include working with Campus Services to i) establish access control recommendations ii) maintain door schedules for the facility or space under their control, iii) document access control and approval, and facilitate the access approval process for faculty, staff, students, affiliates, visitors, and contractors for spaces under their control, and iv) in coordination with Campus Services, will ensure compliance with authorization requirements for access. Also responsible for regularly auditing access to facilities under their control and working with the department head to ensure compliance with this policy.

Physical Access Control Committee: A committee shall be established by the Senior Vice President/Chief Operations Officer of the University, co-chaired by the Associate Vice President of Campus Services and Vice President for Facilities, Campus Development, and Real Estate and will serve in an advisory capacity to Campus Services to review and make recommendations regarding access control and hardware standards as well as best practices on access control processes. The Committee's role will be to review and make recommendations regarding the Physical Access Management Policy, processes and protocols.

Physical Access Control System: Any system or hardware utilized to secure access to a physical location, including facilities, building, spaces, closets, etc. Examples would include, but are not limited to, electronic access systems, keypads, combination lock, metal key locks.

Security Levels

- **Level 1 - "Basic Security":** These areas are typically unlocked during business hours, allowing access by university personnel or the public. After hours these areas are secured; authorized access is by access device(s). University support units will have access to these areas.

- **Level 2 - "Enhanced Security":** Areas that are mechanically and electronically always locked, including during normal business hours, require authorized access device(s) to gain entry each time, and may also require use of PIN. University support units may have access to these areas. This may include residence halls and other enhanced security facilities. Level 2 security may have controls that exceed the controls identified in this policy. Access control for these areas will be maintained by the responsible department in coordination with Campus Services.

- **Level 3 - "High-Risk Security":** Areas that by federal, state, or local laws or code have restricted access, or are restricted by university policies and/or procedures. These areas may require higher security access control devices such as biometric control devices. In most cases access by university support services may be restricted or limited and may require that support services be escorted by approved department personnel. This may include research labs and other high security facilities or areas. High-Risk Security (Level 3) shall have enhanced security controls and access protocols that will exceed the access controls identified in this policy. Access control for these areas will be maintained by the responsible department.

Separation: Any status change which would cause the individual to no longer require or be eligible for physical access to university facilities, buildings, spaces, etc. Example of status changes include, but are not limited to, graduation, retirement, resignation, termination, and death.

8.0 POLICY AND PROCEDURES

8.1 General Access Control

It is the policy of Tulane University to grant, maintain, and revoke physical access to authorized personnel who require access to our facilities, buildings, and spaces based on approved business or mission critical needs.

All requests for physical access to a facility or space must be routed through the DAC and approved based on the Authorization for Access Levels in Appendix 1. All requests for access must comply with the process outlined in in Appendix 2 – Access Issuance Process, Appendix 3 – Key Issuance Process, or Appendix 4 – Key Transfer Process.

All physical access must be issued through Campus Services, including access devices where appropriate. These issued access devices are the property of Tulane University. These issued access devices must be returned or disabled upon termination of employment, completion of contract, graduation, or other separation in accordance with the Access Termination Process in Appendix 6.

Loss or misuse of Tulane University issued access devices may result in the loss of access privileges and/or other disciplinary actions.

All access control systems will maintain compliance with all federal, state, and local laws and University policies, including the Americans with Disabilities Act.

Under no circumstances will any individual install, replace, repair, disable, or override any physical access control system or device including card readers, cores, keypads, or locks without prior approval from Campus Services.

Access to university facilities during scheduled closures such as holidays will default to secure unless otherwise scheduled or requested through Campus Services.

8.2 All Access

Requests for all-access and/or all-access device(s) must be approved in accordance with Appendix 1. Upon approval, all-access/all-access device(s) will be provided by Campus Services.

Employees who are classified as administrators as defined by this policy and employees that work for the following offices, TUPD, Facilities Services, and Enterprise Risk may be granted all access privileges.

Disaster Recovery Teams may be granted all access privileges during or after an emergency. This specialized access will be granted by the Incident Commander or Emergency Operations Center Director and will terminate after the completion of emergency duties.

8.3 Request for Physical Access Control Systems or Hardware

No department, university employee, student or vendor shall purchase, contract, install, or attempt to install physical access control or other high security locking systems without the consent of Campus Services.

Departments shall not modify or discontinue the use of physical access control systems without approval of Campus Services.

8.4 Physical Access Privilege Removal

Upon separation of an individual from the university or department all physical access will be revoked and issued access devices must be turned into the supervisor, department head or issuing department. Interior department access devices may be managed by the DAC with an accurate record of issuance and approval. All changes regarding access device holders must be reported to Campus Services to update the access device control database.

The department head, in coordination with the DAC, is responsible for ensuring all exterior building access devices are returned to Campus Services and verifying that access is revoked.

Failure to obtain access devices from departing individuals and/or lost or stolen access devices provides a security risk to the University. Campus Services is authorized to take appropriate actions as deemed necessary to maintain the security of locations impacted in this manner. The expense of these actions will be the responsibility of the department.

8.5 Monitoring and Review of Physical Access

Physical access controls (video cameras, sensors, etc.) shall monitor physical access to Tulane University where appropriate.

Review of physical access rights shall be performed periodically by the DAC, with a recommendation of quarterly review and no longer than biannually, to review the appropriateness of current access of authorized personnel and remove access that is no longer required.

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.

10.0 APPENDICES

Specific procedures and protocols regarding access granting and terminating access to Tulane facilities are listed below:

Appendix 1. - Authorization Requirements for Access Levels – Campus Services
Appendix 2. - Access Card Issuance Process – Campus Services
Appendix 3. - Key Issuance Process – Campus Services
Appendix 4. - Key Transfer Process – Campus Services
Appendix 5. - New Construction Access Protocol – Campus Services
Appendix 6. - Access Termination Process – Campus Services
Appendix 7. - Additional or Modification of Facility Access Control – Campus Services

11.0 RELATED ACCESS PROCEDURES AND PROTOCOLS

Laboratory Access – Lab Manager and Department Access Coordinator
Emergency Access – Emergency Operations Plan – Office of Emergency Preparedness and Response

Physical Access Management Policy

Appendix 1.

Authorization Requirements for Access Levels

Security Levels	*Space Type*		*Information Type*	*Hazard Type*	*Approvers*
Level 1	A.	Individual Office	Non-Sensitive	Low Hazard	Director
	B.	Office Suites	Non-Sensitive	Low Hazard	Department Head
	C.	Teaching Lab	Non-Sensitive	Low Hazard	Lab Manager
	D.	Storage Areas	Non-Sensitive	Low Hazard	Area Manager
	E.	Other	Non-Sensitive	Low Hazard	Area Manager
Level 2	A.	Individual Office	Sensitive	Low Hazard	Department Head
	B.	Office Suite	Sensitive	Low Hazard	Department Head
	C.	Research Lab	Sensitive	Medium Hazard	Department Head
	D.	Residence Halls	Sensitive	Low Hazard	Residence Hall Director
	E.	Other	Sensitive	Low-Medium Hazard	Department Head
Level 3	A.	Research Labs (Bio, Laser, Rad, etc…)	Sensitive	High Hazard	Department Head/Principal Investigator
	B.	Full Building Access	Any	Any	Vice President(s) or Dean(s)
	C.	All-Access (May exclude specific high hazard or highly sensitive areas)	Any	Any	Sr. VP/COO

Access requests must be made to Campus Services by the DAC after approval as identified in this appendix.

Note: This appendix references the term Department Head as defined by this policy.

Physical Access Management Policy

Appendix 2.

Access Card Issuance Process

- Every employee will receive 24-hour access to the building where their primary office is located.
- Every new employee receives general access to the following areas:
    - Pedestrian gates, front door of the Accounting House (restricted hours), LBC via the LBC Quad and McAlister side, Tidewater (restricted hours), Elks Place, Mail Room, Hutchinson, and Murphy.
- If an employee has a business need to access other spaces, a physical access request form must be completed and submitted to the DAC for approval by the appropriate level approver for the area as indicated in Appendix 1:
    - A clear business need is to be demonstrated in the request.
- After approval, the DAC will submit the form to Campus Services.

Physical Access Management Policy

Appendix 3.

Key Issuance Process

Faculty and Staff:

- If an employee has a business need for key access to other spaces, a key access request form must be completed and submitted to the DAC for approval by the appropriate level approver for the area as indicated in Appendix 1:
    - A clear business need is to be demonstrated in the request.
- After approval, the DAC will submit the key request form to Campus Services.
- Campus Services will open a ticket for an interdepartmental transfer request for key.
- The department will be charged a fee for the key.
- The key is produced and delivered to the requester.

Temporary Key Access:

Other temporary employee access may be granted through Facilities Services supervision and shall be approved based on business need (ie DART team during emergency response). Facilities Services manages and tracks the distribution and return of temporary key access.

Contractors:

For contractors working on Tulane property on a regular basis managers are issued keys based on the business need and they provide access to their employees based on business need.

- Upon request to Campus Services by the Facilities Services Department Head, keys may be issued by the key shop.
- Campus Services opens a ticket for an interdepartmental transfer request for key.
- The department will be charged a fee for the key.
- The key is produced and delivered to the requester.

After-hours access by contractor staff will be controlled by Managers/Supervisors who provide access and ensure the facility is secured after services are provided.

Other temporary contractor access may be granted through Facilities Services Department Head and shall be approved based on business need. Facilities Services manages and tracks the distribution and return of this type of key access.

Contractors that required All-access (O&M):

Preapproved third party contractors may have a business need for temporary 24-hour access to all buildings. This access is granted via key cabinet in Building 85 (fingerprint controlled).

Access to the key cabinet is coordinated by Facilities through IT.

Physical Access Management Policy

Appendix 4.

Key Transfer Process

1. **Keys to level 1 and level 2 spaces which include individual offices or suites may be transferred from one employee to another by the DAC based on the appropriate level of approval as identified in Appendix 1.**

2. **After approval, the DAC must record the key transfer and notify campus services within 48 hours of the key transfer.**

3. **The notification should include the department name, date of transfer, name and title of key receiver, approver name and date of approval and key identification.**

4. **Level 3 keys must be returned to Campus Services upon separation from the university.**

Physical Access Management Policy

Appendix 5.

New Construction Access Protocol

Physical Access Management Policy

Appendix 6.

Access Termination Process

All issued access devices are the property of Tulane University. These issued access devices must be returned or disabled upon termination of employment, completion of contract, graduation, or other separation.

It is the responsibility of the Department Head and DAC to ensure that all access devices are returned or deactivated for areas under their control and that notices of separation are provided to Campus Services.

Physical Access Management Policy

Appendix 7.

Additional or Modification of Facility Access Control