Physical Security for Technology Rooms Policy

Document Number: ITS-0018 **Date Published(sys):** 5/16/2022

General Description

Policy Summary:

This policy is designed to provide the University with a documented and formalized process regarding the access to the Core Infrastructure Data Center and Security Strategy. It regulates access to technology resources by defining "authorized persons", to ensure physical access to the Core Infrastructure Data Center by restricting the access to authorized personnel according to their job roles and responsibilities: safeguarding the facilities and equipment from unauthorized physical access, tampering, theft, and environmental security.

Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity, and availability (CIA) of Trinity University's system components.

Scope:

This policy encompasses all system components that are owned, operated, maintained, and controlled by Trinity University and all other system components, both internally and externally, that interact with these systems.

- Internal system components are those owned, operated, maintained, and controlled by the University and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other system components deemed in scope.
- External system components are those owned, operated, maintained, and controlled by any entity other than Trinity University, but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the description of "Internal system components".
- Trinity applications and systems must be configured to conform as closely as possible to these requirements within the Trinity systems or application's capabilities. For those systems or applications that do not have the capability of enforcing the security controls

mentioned in this policy, an exception must be documented with written permission from the authorized personnel.

Policy Content

Roles & Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees, and users of system components, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to Trinity University information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

- Management Commitment: Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The Chief Information Officer (CIO) is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.
- Internal Employees, Academic Community and Users: Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any University system components. Additionally, users are to report instances of non-compliance to senior authorities, specifically those by other users. Users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of University system components and are to also report such instances immediately to senior authorities.
- Vendors, Contractors and Workforce: Responsibilities for such individuals and organizations are much like those stated for users: adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.

Policy

Trinity University is to ensure that all applicable users adhere to the following guidelines for purposes of complying with the mandated organizational security requirements set forth and approved by management.

Technology Room Access Control

1. Technology rooms should not be easily identified and whenever possible the technology rooms will have a low profile.
2. It is the policy of the University that only Information Technology Services and public safety staff authorized by the Chief Information Officer shall have access to technology rooms.
3. An electronic access control system must be in place and log all access to secure technology rooms. Door access controls must be maintained 24/7 and conform to ISO-27001 standards.
4. Access logs will be maintained for a minimum of one year.
5. Secured doors must default to open in a fire emergency.
6. If an electronic access control system cannot be used then specialized locks that are not part of any standard coring system used on campus may be used, consistent with this policy, including sign-in/sign-out systems.
7. Access to the Data Centers will be provided based on user roles established and agreed by the ITS Core Infrastructure Manager and the ITS TSS Senior Management
    1. The Data Centers employee access will be limited to CIO, ITS Directors, ITS Core Infrastructure Team, ITS Core Infrastructure Security Team and any other ITS personnel identified and documented by ITS Core Infrastructure Manager and approved by the CIO.
8. The University Human Resources organization is responsible for notifying the ITS TSS organization of any University employee termination so ITS TSS can proceed to inform the TigerCard office to limit or terminate the access to the technology rooms upon the notice effectiveness.
9. The ITS Core Infrastructure Manager is responsible for reviewing on a quarterly basis the access to the technology rooms, according to access rights.
10. The ITS Core Infrastructure Manager is responsible to request from the external backup storage provider evidence of the appropriate physical security policy.

Visitors Technology Rooms Access

1. The authorized personnel must ensure that any financial, sensitive confidential or protected employee or student information (e.g., documents, workstation screens) is not visible and is protected from visitor's unauthorized access to such information.
2. No one without proper access may enter a technology room without an ITS escort who is authorized to enter the room.
    1. Authorized visitors must be escorted at all times in any technology room.
    2. Authorized personnel must remain in the technology room until the visitor requiring escort has finished.
    3. All Authorized personnel are responsible for all events during their stay.
    4. Under no circumstance will a contractor be given unsupervised access to technology rooms.
3. The technology room door must remain closed and locked at all times.

Technology Room Equipment Safety

1. The Facilities Services Department must provide a report to ITS once a calendar year on the following elements to ensure the proper functioning and security of the University technology rooms: Smoke Detectors, Fire Alarms, Fire extinguishers, Environmental monitoring system, Air conditioners, Uninterruptible Power supply (UPS).
2. The Tigercard Office is responsible for maintaining a physical security control mechanism at the entrance of the technology room (e.g., card reader) in order to limit access to authorized employees only.
3. The ITS Core Infrastructure Team is responsible to ensure the technology room door is kept closed and locked at all times in order to prevent unauthorized individuals from gaining access to the technology room.
    1. Unsuccessful attempts to gain access to the technology rooms must be monitored.
4. Whenever necessary, the ITS Core Infrastructure Manager is responsible for modifying the established parameters of the environmental monitoring system.
    1. In case of any incident, the system will make automated calls and inform of such incidents as per the identified escalation list.
5. The ITS Core Infrastructure Manager in coordination with Facilities Services must ensure that the technology room has environmental controls that include, but are not be limited to smoke detectors, fire alarms, air conditioner, temperature and humidity controllers, uninterrupted power supply (UPS), power generators, fire extinguishers, and fire suppressant equipment adequate for the information systems housed within the technology room.
    1. Environmental controls must be periodically reviewed and tested, annually or as required, based on the capacity that allows each control for testing
    2. Smoke detectors, fire alarms, air conditioners and fire extinguishers must be in working conditions and must be tested annually by Facilities Services Department or by the external servicing provider to ensure their proper functioning.
6. Controls must be in place to ensure that air quality is properly maintained for the equipment, such as air conditioning, dust filters and associated systems. The technology room must be equipped with a device for monitoring and controlling temperature.
7. The Facilities Services Department is responsible for documenting and providing documentation to ITS for all repairs and modifications to the environmental control mechanisms implemented at the technology room.
8. The ITS Core Infrastructure Team personnel in coordination with their Manager are responsible for periodically reviewing the proper functionality of equipment and other hardware that monitors environmental components.
    1. Monitoring of the proper functionality of equipment and other hardware environmental components are documented within the system logs and alerts are reviewed by the ITS Core Infrastructure team on an ongoing basis.

ITS Stockroom / Storage Room

1. A physical access control method must be established, segregating the IT Storage room from the Technology Room.
    1. Only authorized ITS personnel will have access to the Technology Room as established by the ITS Management.
    2. The ITS TSS Manager is responsible for reviewing on a quarterly basis the access to the ITS Stockroom.

Performance Evaluation

Consequences of Policy Violation:

Any behavior in violation of this policy is cause for disciplinary action and violations of this policy may result in, but are not limited to, any or all the following:

- Loss of university computing, email and/or voice mail privileges
- Disconnection from the residential hall internet network
- University judicial sanctions as prescribed by the student code of conduct
- Reassignment or removal from university housing and/or suspension or expulsion from the university
- Prosecution under applicable civil or criminal laws
- Disciplinary action up to and including immediate suspension or dismissal from position or employment.

Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Contractor	A consultant or independent contractor that enters into an agreement with Trinity University to perform specific services
Electronic Media	Hardware intended to store binary data, e.g., integrated circuit, magnetic tape, or magnetic disk.
Employee	Person working for Trinity University including regular and temporary personnel.
User	Person with privilege to use a system or any resource of information system infrastructure no matter what his/her status (employee or contractor).

Related Documents

Related Content:

This Trinity University *Physical Security for Technology Rooms Policy* is aligned with NIST Special Publication 800-63B, a standardized security framework for Digital Identity Guidelines for Authentication and Lifecycle Management. In addition, this policy is aligned with applicable laws and regulations including HIPAA and FERPA.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v4.0	5/16/2022 3:46 PM	Ben Lim
v3.0	4/19/2022 11:18 AM	Dan Carson
v2.0	1/23/2020 8:30 AM	James Bradley
v1.0	12/4/2019 7:43 PM	Courtney Cunningham

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer