Physical Security for Technology Rooms Policy

General Description

Purpose:
This policy defines standards, procedures, and restrictions for physical access to Trinity University technology rooms. These rooms are also known as IDF or MDF rooms, cabling manholes, data centers, network closets, and a variety of other industry terms for rooms or access points that contain information technology equipment. This policy may also control offices or storerooms where confidential or protected electronic or paper data is stored. The purpose of this policy is to regulate access to Trinity University technology resources by defining "authorized persons."

Scope:
This policy covers all persons and facilities on the Trinity University campus.

Policy Content

1. It is the policy of Trinity University that only Information Technology Services and public safety staff authorized by the Chief Information Officer shall have access to technology rooms.

2. An electronic access control system must be in place and log all access to secure technology rooms. Door access controls must be maintained 24x7 and conform to ISO-27001 standards.

3. Access logs will be maintained for a minimum of one year.

4. Review of procedures and logs must be done annually.

5. Secured doors must fail open in a fire emergency.

6. Where colocation of other equipment or resources cannot be avoided, network equipment and connectivity must be partitioned off through the use of metal fencing or other secured barrier to access and those interior spaces must have access controls consistent with this policy.

7. 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.
8. Semesterly reviews of persons with authorized access to technology rooms must be conducted by the Chief Information Officer or designate.

9. No one without proper access may enter a technology room without an ITS escort who is authorized to enter the room.

10. Under no circumstance will a contractor be given unsupervised access to technology rooms.

Revision Management

Revision History Log:

<table>
<thead>
<tr>
<th>Revision #:</th>
<th>Date:</th>
<th>Recorded By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>v2.0</td>
<td>1/23/2020 8:30 AM</td>
<td>James Bradley</td>
</tr>
<tr>
<td>v1.0</td>
<td>12/4/2019 7:43 PM</td>
<td>Courtney Cunningham</td>
</tr>
</tbody>
</table>

Vice President Approval:

Enter Vice President(s) that are responsible for approving this document

<table>
<thead>
<tr>
<th>Name:</th>
<th>Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gary Logan</td>
<td>Vice President for Finance &amp; Administration</td>
</tr>
</tbody>
</table>