OFFICE OF INFORMATION TECHNOLOGY
Policies and Procedures Manual

1.5. Data Center Access Policy

1.5.1. Approval and adoption

1.5.1.1. Approved by the Chief Information Officer and Executive Vice President and adopted effective 5/3/2007.

1.5.1.2. Updated formatting and content. Reviewed and approved by the Chief Information Officer and Vice President for Facilities & Technology Services and adopted effective 11/1/2017.

1.5.2. Purpose

1.5.2.1. To ensure the safety and confidentiality of the University's enterprise data systems by limiting access to the Data Centers.

1.5.3. Policy

1.5.3.1. Access to the University's Data Centers will be limited to appropriate OIT and Security personnel. Access will be distributed to these individuals only and will be changed on a frequent basis.

1.5.3.2. Under normal conditions, access to the Data Centers by other personnel will be granted and coordinated by OIT personnel regardless of time or day.

1.5.3.3. Under emergency conditions, access to the Data Centers by other personnel may be granted and coordinated by Security personnel regardless of time or day. On these occasions, Security will make every endeavor to contact the appropriate OIT personnel to inform them of the emergency.

1.5.4. Procedure

1.5.4.1. Under normal conditions, University and non-University personnel wishing to access the Data Centers should contact the OIT Help Desk at (909) 448-4130 to request entry. Help Desk personnel should direct the request to appropriate OIT personnel.

1.5.4.2. Under emergency conditions, University and non-University personnel wishing to access the Data Centers should contact Security at (909) 448-4950 and request entry. When contacted and requested to open a Data Center door because of an emergency, Security personnel should:

1.5.4.2.1. Attempt to contact appropriate OIT personnel while they are on their way to provide access;

1.5.4.2.2. Verify an emergency exists;

1.5.4.2.3. Verify the identity of the individual requesting access and their connection to resolving the emergency (e.g. police responding to a bomb threat, firefighters responding to a fire alarm, HVAC personnel responding to a temperature alarm, etc.);

1.5.4.2.4. Remain with the third-party during the time access to the Data Center is granted or get another ULV staff member to do so if Security must leave for another emergency;

1.5.4.2.5. Log the information (date, time, name, reason, etc.);

1.5.4.2.6. Email a report of the incident to the Senior Director of Campus Safety, Senior Director of Infrastructure Support, and the Chief Information Officer at their first opportunity following the emergency.

1.5.5. Enforcement

1.5.5.1. Violations of any part of this policy may result in disciplinary action as prescribed by University policies and procedures.