Data Center Terms of Access

ACCEPTANCE OF TERMS AND CONDITIONS FOR ACCESS

The following are the terms of access for all customers who use or require access to the Computing & Information Services (CIS) Data Center(s) and/or Other Secure Areas associated with the data center(s). By accessing, and/or using the CIS Data Center(s), you acknowledge having read, and understood these terms. By clicking the "I have read the Data Center Terms of Access…" statement in the Badge/Card Access Request System, you are acknowledging your adherence to these terms. Failure to comply with these terms may result in the loss of your access to the CIS Data Center.

RENEWAL PROCEDURES

Full-time CIS employees: Access authorization must be renewed annually during the announced renewal period. Full-time TAMU employees (not employed by CIS): Access authorization must be renewed annually during the announced renewal period.
Student Workers and Vendors: The access renewal process will occur three times per year near semester boundaries.
Data Center badge access reports are run every 30 days. Anyone who has not accessed the facilities during the 30 day period will have their access deleted. A new request must be submitted through BARS if access to the facilities is needed again.

USE RESTRICTIONS

Physical access authorization to the machines located in the CIS Data Center(s) is maintained and provided by CIS. Except as stated herein, none of the machines located in the CIS Data Center(s) may be removed, installed, or modified in any form or by any means (including, but not limited to remote network access) without the prior permission of the respective system owner(s) and CIS.

REMOTE ACCESS ENCRYPTION / SECURITY

For systems located in the CIS Data Center(s), establishing remote access capability will be a coordinated effort involving the CIS Network Group and the appropriate system administrators. System administrators must contact the CIS Network Group to establish remote access capability for their systems.

RULES OF CONDUCT

As a user of the CIS Data Center(s), you must abide by the following Rules of Conduct. Additionally, you agree that, as a user of the CIS Data Center(s), you will comply with all requests made by the CIS Operations Group concerning the CIS Data Center(s), and will abide by the following protocols:

- Badges/ID Cards issued or authorized by CIS for access to the data center(s) are not to be shared and must be worn (and visible) at all times while in the CIS Data Center(s). Persons found not to be wearing an authorized badge/ID card will be asked to leave. How are you currently addressing this problem?
- Equipment should be in its designated place unless currently undergoing repairs or removal.
- Tools or diagnostic equipment should be stored away when not in use.
- Aisles should be kept free of materials, including: wiring, cables, and other related materials. An aisle width of 4 feet should be maintained.
- Whenever possible, equipment should be unpacked and shipping materials removed before the item is moved to the CIS Data Center(s). This will help reduce the accumulation of clutter and trash. Each group will be responsible for packing materials taken into the CIS Data Center(s) and should remove such materials promptly.

- "Cleanup Day" – on designated days and times, all groups that have support roles for systems in the CIS Data Center(s) will work together in a cleanup/policing of the CIS Data Center(s). The Operations Group will schedule, announce, and supervise these "cleanup" days.
- Any items (cartons, crates, containers) found in the CIS Data Center(s) that have not been properly checked in with Operations personnel and labeled, will be removed by the Operations personnel. Permanent items should be placed in locked cabinets.
- Food and Drinks ARE NOT permitted in the CIS Data Center(s).
- Operations personnel will make routine inspections of the CIS Data Center(s) to maintain the appropriate environment and promote proper procedures.
- Violation of these rules could result in the immediate revocation of access to the CIS Data Center(s) and may result in liability for damages.

SECURITY CONSIDERATIONS

Reasonable precautions have been exercised in securing the CIS Data Center(s) to prevent unauthorized access or tampering with mission critical systems and data. Personnel desiring continued access are required to register and obtain a photo ID badge from the TAMU badging office. They are requested to maintain the confidentiality of their photo ID card/badge and report lost or stolen cards/badges immediately to Help Desk Central. Photo ID cards/badges are to be worn at all times when in the CIS Data Center(s). All individuals who plan to have continued access the CIS Data Center(s) are required to have his or her own unique photo access ID card/badge, except as stated below.

Visitor/Guest Badges/ID Cards are to be worn at all times by those individuals who are visitors/guests when visiting the CIS Data Center(s). Visitor/Guest Badges can be obtained from Help Desk Central. Visitors/guests will be asked to sign a visitor's log and leave a photo ID (e.g. Driver's License) which will be returned upon check-in of visitor badge.

ESCORT PROCEDURES

Visitors and Guests must be escorted at all times by a full-time TAMU employee with authorized access while in the CIS Data Center(s). Vendors (from outside TAMU) who need access to the CIS Data Center(s) will sign for special Vendor badges at Help Desk Central. An escort from an access-authorized member of the hosting group (support personnel for the particular resource) or the CIS Operations group is required.

SECURITY STATEMENT

By acknowledging that you have read these terms and agree to abide by them, you understand that if you violate University regulations and / or State and Federal laws by gaining unauthorized access to the CIS Data Center(s) and / or systems therein, you will be subject to University disciplinary action and criminal prosecution to the full extent of the law (Chapter 33, Title 7 of the Texas Penal Code). You also acknowledge that neither you nor anyone else possesses the authority to allow anyone to use your ID and password. In addition, you agree not to attempt to circumvent the computer security system(s) by using or attempting to use any software, files, or resources that you are not authorized to use. Your acceptance of the terms of this document remain in effect for the entire time for which you have access (granted or renewed) to the CIS Data Center(s) or until you agree to a subsequent CIS Data Center(s) Terms of Access document.

CONTACT INFORMATION

If you have any questions or comments about the terms of access or the conditions specified above, please direct them to the Associate Director of CIS Operations and Customer Help and/or Help Desk Central at 979-845-8300.