User Guidelines for Data Center and Communication Room Access

Guideline No.	ITS-1013-G	Rev	F
Owner:	IT Security and Compliance		
Approved by:	Sheryl Okuno, Director		
Issued:	5/30/08	Revised:	9-26-13
			Page 1 of 10

Table of Contents

1. Purpose

Information Technology Services (ITS) is responsible for the centralized data center and campus communication rooms that house servers, network equipment, voice and data equipment, disk storage subsystems, workstations, tape backup systems, and other campus administrative computing and communications systems that may contain Level 1 or Level 2 confidential data. Access to the centralized data center and communication rooms is strictly controlled and limited only to authorized personnel. These guidelines outline the requirements for obtaining authorized access to the data center and communication rooms.

2. Entities Affected by This Guideline

This guideline applies to all individuals authorized to access the data center and/or communications rooms including, but not limited to, ITS employees, University employees responsible for the installation, use or maintenance of equipment housed in the restricted area, and all third-party service providers who must enter the area to install, repair or maintain equipment or systems housed therein.

Note: Department administrators are responsible for user and physical access controls to decentralized systems located outside of the centralized data center and not managed by ITS. See *ITS-2011-S User Access Control for Decentralized Systems* for more information.

3. Definitions

a) Accompany: To go with, remain with and monitor the actions of another.

b) Authorized Personnel: Individual(s) who is (are) granted access privileges to restricted areas, equipment, systems or data following formal review and approval of the legitimate business purpose for such access.

c) Breach: Infraction or violation of a law, regulation, guideline, policy or standard.

d) Communications Rooms: Secured rooms containing communications equipment including, but not limited to, telephone systems (PBXs), voice mail systems, call collection computers, cable plant, wired and wireless network equipment, servers and termination blocks.

e) Data Center: Secured rooms containing computing equipment including, but not limited to, computers, servers, printers, environmental equipment and other related computing equipment. The centralized data center is managed by Information Technology Services (ITS).

f) Decentralized System: Any data system or equipment containing data deemed private or confidential or which contains mission critical data, including departmental, divisional and other ancillary system or equipment that is not managed by central ITS.

g) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.

h) Level 2 Internal Use Data: Internal use data is information that must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

i) Standard Access: Non-temporary access to restricted computing and communications areas granted to individuals whose job responsibilities require such access on an ongoing or daily basis.

j) Temporary Access: Limited, monitored access to restricted computing and communications areas granted to individuals who may from time-to-time have a business need for such access.

k) Third-party Service Provider: Refers to an entity that is undertaking an outsourced activity on behalf of the University or is performing system administrator duties on their offsite system that contains University protected data (e.g., vendors, vendor's subcontractors, business partners, consultants, etc.).

4. Guidelines

4.1 Requesting Data Center or Communication Room Access

CSULA employees and, under special circumstances as outlined in 4.2.3, third-party service providers can request standard or temporary access to the data center, switchroom, telephone closets or other communications rooms managed by ITS by completing form *ITS-8825 Data Center/Communications Access Request*. All applicants must adhere to the User Responsibilities and Appropriate Use of Access Agreement contained therein.

4.2 Requirements for Data Center or Communication Room Access

Only CSULA employees, as well as third-party service providers under contract to the University, whose job duties meet the applicable criteria below may be granted access privileges to data centers and communication rooms.

Departments are responsible for notifying the director of IT Security and Compliance when employment changes occur that require a revocation of access. (See section 4.3.1 c) below.)

4.2.1 Criteria for Data Center Access

Standard access to data centers is limited to only those whose job duties legitimately require that the work to be performed, and can only be so performed, in the data center.

Authorized personnel with an ongoing legitimate business need for data center standard access would include the following:

- Vice president for ITS and chief technology officer
- All ITS directors
- Selected ITS management who cannot perform a required job function(s) in any other location
- ITS network personnel
- ITS server personnel
- ITS computer operations personnel
- Library personnel whose job duties require maintenance of Library systems that run only on computer room computers or servers.
- Administrative Technology personnel whose job duties require maintenance of Administration and Finance systems that run only on computer room computers or servers.
- Information Technology Consultants (ITCs) whose job duties require maintenance of academic or administrative systems that run only on data center computers or servers.

A list of approved personnel authorized for standard access shall be posted prominently in the data center. Only individuals whose names appear on this list may enter the data center unaccompanied. Other individuals must be accompanied by one or more persons whose names are on the authorized standard access list. (See item 4.2.2 a) below.)

Other individuals who may from time-to-time have a business need for data center access may be granted temporary access to such rooms. These individuals ***must be accompanied*** by one or more persons with standard access, and ***must sign in and out*** on the *ITS-7804 Data Center/Switchroom Access Log*. Individuals who may be granted temporary, monitored access include:

- Cal State L.A. Facilities Operations employees
- Facilities Services outside vendors (e.g., air conditioner repair)
- Third-party service providers contracted by the ITS

Individuals who do not have a business need for data center access ***may not enter*** such rooms under any circumstances. Those individuals with standard access to a data center ***may not accompany*** anyone who does not have a legitimate business need to be in such a room.

4.2.2 Criteria for Communication Room and Switchroom Access

a) Standard access to communications rooms and the switchroom may be granted only to the following levels of ITS staff:

   a. Vice president for ITS and chief technology officer
   b. Director of IT Infrastructure Services
   c. Assistant director of Network Operations Center, Servers and Technology Operations
   d. Manager of Network and PBX Operations
   e. Network technicians
   f. Telecommunications technicians

b) <u>Temporary access</u> may be granted to individuals who have a business need from time-to-time to work in the switchroom or communication room. Individuals granted temporary, monitored access ***<u>must be accompanied</u>*** by one or more persons with standard access. Individuals who may be granted temporary access include:

a. Cal State L.A. Facilities Operations employees
b. Facilities Services outside vendors (e.g., air conditioner repair, etc.)

4.2.3 Criteria for Third-party Service Provider Access

a) <u>Standard access</u> to the data center, communications rooms and the switchroom is generally not allowed to third-party service providers. However, standard access may be granted to third-party service providers who are contractually assigned to the campus as a “full-time” service provider. These vendors are required to submit *ITS-8825 Data Center/Communication Room Access Request* for approval and, following approval, may access the rooms unaccompanied. Vendors must comply with this guideline and the Appropriate Use of Access Agreement contained in ITS-8825. This standard access is limited to the duration stated in the University contract or service order. These vendors who may be granted standard access include:

- PBX maintenance vendor
- Any vendor or consultant assigned to the campus on a daily, full-time basis, but for an extended, contractually defined period of time, to perform contracted work.

b) <u>Temporary access</u> may be granted to third-party service providers contracted by ITS for a specific maintenance or installation activity. To enter the data center or communications room, and to handle its contents, third-party service providers must sign in and out on the ITS-7804 access log and be accompanied by authorized University employees.

4.2.4 Emergency Personnel

It is understood that there may be the need for personnel to access an area in case of an emergency (e.g., fire, police, medical, etc.). In this case, access is granted only for the purpose of responding to the emergency and with immediate notification to the vice president for ITS.

4.3 Responsibilities Concerning Data Center and Communication Room Access

4.3.1 Department or Unit Manager

Department and unit managers are responsible for the following:

a) Evaluating data center or communication room access applications. Approve applications only where an applicant’s job title, employment responsibilities and stated justification meet the criteria for allowing data center or communication room access.

b) Approving applications only where an applicant’s job title, employment responsibilities and stated justification meet the criteria for allowing data center or communication room access.

c) Immediately notifying IT Security and Compliance at <u>ITSecurity@calstatela.edu</u> in any of the following situations:

- An individual’s job duties no longer require access to a data center or communication room, including separation from the University.
- A third-party service provider’s contract expiration.
- If there is any reason to revoke or modify an individual’s access to a data center or communication room.

4.3.2 ITS Management

a) The vice president and CTO; director of IT Security and Compliance; director of IT Infrastructure; assistant director of Network Operations Center, Servers and Technology Operations and the manager of Network and PBX Operations shall evaluate all data center and communication room access applications. Approve applications only where an applicant's job title, employment responsibilities and stated justification meet the criteria for allowing data center and communication room access.

b) The assistant director of Network Operations Center, Servers and Technology Operations shall verify which rooms and equipment an applicant is approved to access and handle.

c) The assistant director of Network Operations Center, Servers and Technology Operations shall regularly audit the list of those with authorized access to data centers and communication rooms to ensure the list is current and accurate. Remove access for any individuals whose status and job responsibilities do not justify it.

d) The assistant director of Network Operations Center, Servers and Technology Operations shall visibly post the most current log of users with data center and communication room access. Logs must be updated and reposted as changes occur. Handwritten deletions or additions to the posted logs are not acceptable compliance standards. The logs should be retained for a period of one year for audit compliance.

e) The assistant director of Network Operation Center, Servers and Technology Operations shall either e-mail the updated log of approved users to all ITS managers or post the log of approved users on SharePoint for access by all ITS managers. A current electronic list of approved users must be available to all ITS managers for verification at all times to prevent physical alternation of the posted log.

4.3.4 ITS Staff

a) Process *ITS-8825 Data Center/Communication Room Access Request* form.

b) Maintain a secured record of users and their OmniLock codes.

c) Authorize the creation of Golden Eagle Card PINs and OmniLock codes for approved users.

d) Create OmniLock codes for approved users.

e) Notify approved users when their access information is ready to pick up at ITS Help Desk or the One Card office.

f) Verify approved users' Golden Eagle Cards and signatures prior to issuing OmniLock codes.

4.3.5 One Card Office

a) When directed by the assistant director of Network Operations Center, Servers and Technology Operations, create encrypted Golden Eagle Card PINs for approved users.

b) Maintain a record of users who have been assigned Golden Eagle Card PINs.

c) Verify users' Golden Eagle Cards and signatures prior to issuing Golden Eagle Card PINs.

4.3.6 Individuals with Authorized Access to Data Centers and Communication Rooms

a) Adhere to all the terms and conditions agreed to on *ITS-8825 Data Center/Communication Room Access Request*.

b) Do not identify an access code or PIN as being connected with any data center or communications room.

c) Do not leave an access code or PIN where anyone else can find, view or copy it.

d) Do not allow entry to a data center or communication room to any other individual, except when given permission by the assistant director of Network Operations Center, Servers and Technology Operations to accompany individuals who have been granted temporary access.

e) Immediately report any unauthorized access to the following individuals in the order specified below:

- The assistant director of Network Operations Center, Servers and Technology Operations
- Director of IT Infrastructure Services
- Director of IT Security and Compliance
- Vice president for ITS and CTO

4.4 Responsibilities Concerning Data Center and Communication Room Use and Safety

a) Doors to secured areas may never be propped open. Individuals leaving the data center or communication room are responsible for ensuring the room is fully secured before departing. Exceptions may be granted by the director for IT Infrastructure or the assistant director of Network Operations Center, Servers and Technology Operations under the following conditions:

- Environmental problems leading to excessive temperatures place the equipment or operating conditions in jeopardy.
- Work being performed by staff or third-party service providers requires open access, e.g., equipment transport, external power provision, temporary cable to an external location, etc.
- The location is monitored by an authorized individual at all times to prevent unauthorized access.

b) ITS will comply with all published University safety and risk management practices issued by Risk Management/Environmental Health and Safety related to environmental controls, chemicals and combustible materials storage and safety, and occupational safety.

c) All individuals will comply with Administrative Procedure 006, University Smoking Policy.

d) Food and drink are not allowed in the data center machine room or communications rooms.

e) Food and drink are allowed, but not recommended, in the data center console room and the switchroom office area. Individuals working in these areas are responsible for ensuring their careful consumption and the cleanliness of the work area.

f) Chemicals, cleaning supplies and combustible materials may not be stored in the data center or communications room.

g) Combustible materials, such as papers, empty boxes, rags and the like, may not be stored in the data center or any communications rooms.

4.5 Reporting Theft and Security Breaches

a) **Immediately, within 15 minutes of discovery, report the theft of any data center or communication room contents** to: University Police at 323-343-3700, Department of Public Safety, Building 46. If a computer or any other electronic storage device is among the stolen contents, fill out *ITS-2804 Lost or Stolen Computer or Electronic Storage Device Report* obtained from University Police or online. Submit the completed form to IT Security and Compliance immediately: E-mail it to ITSecurity@calstatela.edu or bring it to the ITS Help Desk (LIB PW Lobby).

b) **Immediately**, **within 15 minutes of discovery**, **report any security breaches or violations of campus or remote CMS databases** by phone to the individuals listed below. A written follow-up minimally containing the date, time, event, emergency contact personnel, emergency contact phone number, system impact, user impact, current actions and planned actions, must be e-mailed to the same individuals **within four hours of discovery**.

Vice President for Information Technology Services and CTO Phone: 323-343-2600 ITSecurity@calstatela.edu	Director of IT Security and Compliance Phone: 323-343-2600 ITSecurity@calstatela.edu

c) The vice president for Information Technology Services/CTO and the director of IT Security and Compliance are responsible for notifying University Counsel **within 30 minutes of discovery** and providing periodic updates as required.

d) All security breaches and violations shall be investigated forthwith, by the director of IT Security and Compliance following the protocols outlined *in ITS-2511 Campus Security Incident Response Team (CSIRT)*.

e) The final report(s) regarding all security breaches shall be filed with the director of IT Security and Compliance.

4.6 Reporting Unauthorized Access

a) **Immediately** report any unauthorized access to the individuals, and in the order specified, below:

- Assistant director of Network Operations Center, Servers and Technology Operations
- Director of IT Infrastructure Services
- Director of IT Security and Compliance
- Vice president for ITS and CTO

4.7 Annual Review of Approved Access

a) The director of IT Security and Compliance is responsible for conducting an annual review of approved access. The review must be completed during the fall academic quarter.

b) The annual review shall consist of verifying those with authorized standard access, Golden Eagle Card PINs and OmniLock codes.

c) The assistant director of Network Operations Center, Servers and Technology Operations shall correct any findings of unauthorized access within 24-hours.

5. Contacts and Resources

a) Report problems accessing the Data Center/Communication Room Access Request form to the ITS Help Desk at 323-343-6170.

b) Address questions regarding these guidelines to: ITSecurity@calstatela.edu.

Related Documents

CSULA	Title
ITS-2524	**Cal State L.A. Information Security Program** http://www.calstatela.edu/its/itsecurity/guidelines/Campus_Information_Security_Plan_2012.pdf This document establishes the University's Information Security Program in support of its obligation to protect the technology resources and information assets entrusted to it.
ITS-2511	**Campus Security Incident Response Team** This internal document, available from the director for IT Security and Compliance, defines the steps to effectively respond to information security incidents, minimize disruption and return operations to a normal state.
ITS-2804	**Lost or Stolen Computer or Electronic Storage Device Report** http://www.calstatela.edu/its/forms Form used to report a lost or stolen computer or electronic storage device to University Police and IT Security and Compliance.
ITS-7804	**Data Center/Switchroom Access Log** Internal ITS form, available from the assistant director of Network Operations Center, Servers and Technology Operations, is used to record entry and exit from the data center or communications room.
ITS-8825	**Data Center Access Request** http://www.calstatela.edu/its/forms Form used to apply for access to the data center and communication rooms.
Chancellor's Office	**Title**
CSU Information Security Policy	**The California State University Information Security Policy** http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies governing CSU information assets.