 <b>User Guidelines for Data Center/Communication Room Access</b>	No.	ITS-1013-G	Rev	E
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	5/30/08	Effective:	5/30/08
	Page 1 of 6			

## 1 Purpose

Information Technology Services (ITS) is responsible for the campus data centers and 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 confidential, personal, and/or proprietary information. Access to data centers and communication rooms is strictly controlled and limited only to authorized personnel. These guidelines outline the requirements for obtaining authorized access to data centers and communication rooms.

## 2 Definitions

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

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

**Confidential Information:** In addition to the personal information listed below, examples of confidential information include the following: financial records, student educational records, physical description, home address, home phone number, grades, ethnicity, gender, employment history, performance evaluations, disciplinary action plans, or NCAA standings. Confidential information must be interpreted in combination with all information contained on the computer to determine whether a violation has occurred.


**Health Insurance Information:** An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records

**Medical Insurance Information:** Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional

**Personal Information:** The California Personal Information Security Act (SB 1386) and Confidentiality of Medical Information Act (AB 1298) define personal information as: An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number
- Driver's license or California Identification Card number
- Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Medical information
- Health insurance information

**Proprietary Information:** Information that an individual or entity possesses, owns, or holds exclusive rights to. Examples include: faculty research, copyrighted materials, white papers, research papers, business continuity and other business operating plans, e-mail messages, vitae, letters, confidential business documents, organization charts or rosters, detailed building drawings, and network architecture diagrams. Proprietary information, if lost or stolen, could compromise, disclose, or interrupt operations or embarrass the individual or the University.

 <b>User Guidelines for Data Center/Communication Room Access</b>	No.	ITS-1013-G	Rev	E
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	5/30/08	Effective:	5/30/08
	Page 2 of 6			


## 3 Guidelines

### 3.1 Requirements for Data Center/Communication Room Access

Only Cal State L.A. employees, as well as vendors and consultants under contract to the University, whose job duties meet the applicable criteria below may be granted access privileges to data centers and communication rooms.

#### 3.1.1 Criteria for Data Center (Computer Room) Access

- a) Standard (i.e., non-temporary) 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 a computer room.
- b) Authorized personnel with an ongoing legitimate business need for data center standard access would include the following:
  - Vice President, 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/servers.
  - Administrative Technology personnel whose job duties require maintenance of Administration and Finance systems that run only on computer room computers/servers.
- c) A list of approved personnel authorized for standard access shall be posted in the data center. Only individuals whose names appear on this list may enter the data center. Otherwise, they must be accompanied by one or more persons whose names are on the list. (See item 3.1.1 d) below.)
- d) Other individuals who may from time to time have a business need for data center access may be granted temporary, monitored 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 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)
  - University Police with a master key, and only in case of emergency, and only with prior approval from the ITS VP.
- e) Individuals who do not have a business need for computer room access may not enter such rooms under any circumstances. Those individuals with standard access to a computer room may not accompany anyone who does not have a legitimate business need to be in such a room.

 <b>User Guidelines for Data Center/Communication Room Access</b>	No.	ITS-1013-G	Rev	E
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	5/30/08	Effective:	5/30/08

Page 3 of 6

### 3.1.2 Criteria for Communications Room and Switchroom Access

- a) Standard access to communications rooms and the switchroom may be granted only to the following levels of ITS staff:
  - Vice President, ITS and Chief Technology Officer
  - Director, IT Infrastructure Services
  - Assistant Director, Network Operations Center, Servers, and Technology Operations
  - Director, Financial and Support Services
  - Network technicians
  - Telecommunications technicians
- b) Temporary, monitored access may be granted to individuals who have a business need from time to time to work in a data center or communication room. Individuals granted temporary, monitored access must be accompanied by one or more persons with standard access. 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, etc.)
  - University Police with a master key, and only in case of emergency, and only with prior approval from the ITS VP.


## 3.2 Responsibilities Concerning Data Center/Communication Room Access

### 3.2.1 Department Chair or Unit Manager

- a) Evaluate data center/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) Immediately notify IT Security and Compliance at [ITSecurity@calstatela.edu](mailto:ITSecurity@calstatela.edu) in any of the following situations:
  - An individual's job duties no longer require access to a data center or communication room
  - A vendor's or consultant's contract expires
  - If there is any reason to revoke or modify an individual's access to a data center or communication room

### 3.2.2 ITS Management

- a) The Vice President and CTO; IT Security and Compliance Director; and the Assistant Director of Network Operations Center, Servers, and Technology Operations should evaluate all data center/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 should designate which rooms and equipment an applicant is approved to access and handle.
- c) The Assistant Director of Network Operations Center, Servers, and Technology Operations should regularly audit the list of those with authorized access to data centers and

 <b>User Guidelines for Data Center/Communication Room Access</b>	No.	ITS-1013-G	Rev	E
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	5/30/08	Effective:	5/30/08
	Page 4 of 6			

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 should maintain and visibly post a log of users with data center/communication room access.

### 3.2.3 ITS Staff


- a) Process 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 and/or the One Card office.
- f) Verify approved users' Golden Eagle Cards and signatures prior to issuing OmniLock codes.

### 3.2.4 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.

### 3.2.5 Individuals with Authorized Access to Data Centers and/or Communication Rooms

- a) Adhere to all the terms and conditions agreed to on the 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 individuals, and in the order specified, below:
  - The Assistant Director of Network Operations Center, Servers, and Technology Operations
  - Director, IT Infrastructure Services
  - Director, IT Security and Compliance
  - ITS Vice President and CTO

 <b>User Guidelines for Data Center/Communication Room Access</b>	No.	ITS-1013-G	Rev	E
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	5/30/08	Effective:	5/30/08
	Page 5 of 6			

### 3.3 Reporting Theft and Security Breaches


- a) **Immediately** report the theft of any data center or communication room contents to: University Police at (323) 343-3700, Department of Public Safety, Building C. If a computer or any other electronic storage device is among the stolen contents, fill out the Lost or Stolen Computer or Electronic Storage Device Report obtained from University Police. Submit the completed form to IT Security and Compliance immediately: E-mail it to [ITSecurity@calstatela.edu](mailto: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** 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**.

VP, Information Technology Services and CTO Phone: 323-343-2600 <a href="mailto:ITSecurity@calstatela.edu">ITSecurity@calstatela.edu</a>	Director, IT Security and Compliance Phone: 323-343-2600 <a href="mailto:ITSecurity@calstatela.edu">ITSecurity@calstatela.edu</a>
--	---

- c) The Vice President, Information Technology Services and CTO, as well as the Director, 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, followed up with a report containing analysis of the matter and recommendations for action. The database administrator and the Director of IT Infrastructure Services are responsible for addressing all campus action items. The Director of CMS and Enterprise Systems is responsible for addressing all CMS action items.
- e) The final report(s) regarding all security breaches shall be filed with the Director, IT Security and Compliance.

### 4 Terms, Conditions, and Sanctions

- a) The violation of security precautions for the protection of personal and confidential information may be a crime and may be subject to appropriate legal action and/or criminal prosecution.
- b) A violation may furnish the basis for disciplinary as set forth by statute, including but not limited to Education Code section 89535, up to and including dismissal.
- c) The illegal use of data, computers, programs, systems, networks, or supporting documentation is a violation of Penal Code Section 502 and is punishable by fine and/or imprisonment.
- d) Vendors or consultants in violation of the herein guidelines will lose access privileges, and the vendor's/consultant's company will be disqualified from Cal State L.A. bids, purchase orders, contracts, and awards for a period of two (2) years.
- e) California Senate Bill (SB) 1386 and Assembly Bill (AB) 1298 requires the campus to notify all affected individuals when their unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

 <b>User Guidelines for Data Center/Communication Room Access</b>	No.	ITS-1013-G	Rev	E
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	5/30/08	Effective:	5/30/08
	Page 6 of 6			

## 5 Contacts and Resources

- a) To report a security breaches or violations, contact IT Security and Compliance at: (323) 343-2600, LIB PW 1070, [ITSecurity@calstatela.edu](mailto:ITSecurity@calstatela.edu).
- b) Report the theft of any data center and/or communication room contents, immediately to University Police, (323) 343-3700, Department of Public Safety, Building C.
- c) **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, IT Infrastructure Services
  - Director, IT Security and Compliance
  - ITS Vice President and CTO
- d) Report problems accessing the Data Center/Communication Room Access Request form to the ITS Help Desk at (323) 343-6170.
- e) Address questions regarding these guidelines to: [ITSecurity@calstatela.edu](mailto:ITSecurity@calstatela.edu).

## 6 Related Documents

ID/Control #	Title
ITS-8825	<b>Data Center Access Request</b> Form used to apply for access to the data center and communication rooms <a href="http://www.calstatela.edu/its/forms">http://www.calstatela.edu/its/forms</a>
ITS-7804	<b>Data Center/Switchroom Access Log</b> Internal ITS form used to record entry and exit from the data center or communications room ITS Help Desk, LIB PW Lobby
ITS-2804	<b>Lost or Stolen Computer or Electronic Storage Device Report</b> Form used to report a lost or stolen computer or electronic storage device to University Police and IT Security and Compliance <a href="http://www.calstatela.edu/its/forms">http://www.calstatela.edu/its/forms</a>