Data Center Access Policies and Procedures

Version 2.0
Tuesday, April 6, 2010
Table of Contents

UITS Data Center Access Policies and Procedures 3

Introduction.3

Overview 3

Data Center Access 3

Data Center Access - Levels of Access 4

Periodic Review and Termination of Access 5

Data Center Access Log 5

Access Exception Reporting 5

Appendix A: Data Center Access Agreement.6

Appendix B: Data Center Unescorted Access Request Procedure 7

Appendix C: Data Center Etiquette 8

Appendix D: Data Center Approved Vendor Access Procedure 9
UIT Data Center Access Policies and Procedures

Introduction
The UITS Data Centers provide stable environments, enhanced security, fire suppression equipment and alarms, uninterrupted power (UPS and generators), high-speed network connectivity, 24x7 Operator coverage and other features required by the mission-critical resources they contain. The policies and procedures described in this document have been developed to maintain a secure, safe environment and must be followed by individuals working in or visiting the Data Centers. All individuals requesting access or maintaining servers in the Data Center must understand and agree to these procedures.

Overview
The UITS Data Centers contain the University of Arizona’s enterprise computing and networking resources. Access is controlled to protect both the physical resources and the enterprise data from unauthorized use, accidental or malicious damage and theft. Access to the Data Centers will only be granted when a legitimate business need is demonstrated. This access policy and procedure document specifies the criteria for granting access to specific individuals or groups. Failure to follow these policies is considered grounds for dismissal and/or prosecution. Failure of a vendor, consultant, or contractor to follow these policies is grounds for termination of agreements and subsequent legal action. Any questions regarding policies and procedures should be addressed to the UITS Infrastructure Services Operations Center (ISOC) Assistant Director. This Data Center Access Policy may be suspended in the event of an emergency that requires access for medical, fire, or police personnel.

Data Center Access
CatCard swipe access and unsupervised 24x7 access to the Data Centers will only be given to individuals with an approved and demonstrated business need to access the Data Centers on a regular basis, those individuals requiring infrequent access will be granted escorted access as needed. Individuals with unescorted access may escort and supervise unauthorized individuals provided all individuals are logged on entry and exit. CatCards belonging to authorized individuals may not be loaned to unauthorized individuals; such action is grounds for disciplinary action. There are no temporary or ‘blank’ access cards available. Any employee or vendor that forgets or misplaces their CatCard will be restricted to escorted access to the Data Centers until their CatCard is replaced.

Violations of the agreement can result in removal of access. Individuals that violate the policies and are removed from the list may face additional disciplinary actions, pending review by the responsible ISOC Assistant Director.
Data Center Access - Levels of Access

A. Escorted
Individuals that have an infrequent need for Data Center access will be granted Escorted status and will not have CatCard swipe access. Escorted access will be provided primarily during normal business hours. Data Centers that do not have 24x7 Operations coverage will have after-hours escorted access on an emergency or pre-arranged basis only. Individuals requesting escorted access must be signed in and out in the Data Center access log by a member of the ISOC staff. They are required to provide identification on demand and leave the facility when requested to do so. They must not allow any other person access to the Data Center.

B. Unescorted
Employees that work inside the Data Center and other individuals that have been granted the access based on their job requirements and a demonstrated legitimate business need will have 24/7 access to the Data Center. CatCards must be visible at all times when in the Data Center. Please see Appendix B: Data Center Unescorted Access Procedure on page 7 for more information.

C. Vendor
Approved vendors with CatCards may be granted unescorted access to the Data Center to perform scheduled maintenance or repair work. Vendors not approved for unescorted access may be granted escorted access. Please see Appendix D: Data Center Approved Vendor Access Procedure on page 9 for information about vendor access.

D. Data Center Tours
Tours must be pre-approved by the ISOC Assistant Director. All visitors must sign in and out and must be escorted while touring the Data Centers.

E. Maintenance and Custodial Staff
University maintenance and custodial staff will need to be escorted when accessing the Data Centers. All facilities staff must sign the access log upon entering and leaving the Data Center and inform the ISOC staff of any maintenance work. The ISOC staff must enter any maintenance work in the operations log.

F. First Responders
Campus first responders are granted unescorted access. The list of campus first responders is provided to Amer-X by the UAPD.
Periodic Review and Termination of Access
The ISOC Assistant Director will review the access list every 90 days and will remove any individuals who no longer have a legitimate business need to access the Data Centers. The UITS CIO office will review the access list quarterly.

As part of the employee exit procedure the ISOC staff is notified when employees leave the department. The ISOC Manager will request the immediate removal of access rights if the employee has Data Center access.

Data Center Access Log
The Access logs at each Data Center must be maintained at all times by the ISOC staff. All escorted individuals entering the Data Center must sign the log as they enter and exit for audit purposes.

Access Exception Reporting
Any unauthorized access to the Data Center must be logged by the Data Center Staff in the daily operations log and must be reported to the on-duty ISOC Manager who will determine if the incident needs to be reported to the campus police.

Attempts to forcibly enter the Data Center must be immediately reported to campus police. The on-duty ISOC Manager must also report the incident in writing to the ISOC Assistant Director.

Data Center Etiquette Rules
It is mandatory that all people working within the Data Center adhere to the posted rules of etiquette. This will insure Data Center safety and efficiency.

Please see Appendix C: Data Center Etiquette on page 8 for more information.
Appendix A: Data Center Access Agreement

Applicant Name: ________________________________________________________________
Applicant Email: ___________________________ CatCard#: __________________________
Applicant Department: __________________________________________________________
Office Phone: ___________________________ Emergency Contact Phone: ________________
Supervisors Name: _____________________________________________________________
Supervisors Email: ______________________________________________________________

Justification for Access:
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________

Requested Access:
UITS Site 1 Data Center □ UITS Site 2 Data Center □ Switch Room Data Center □ Research Data Center □

Those granted Data Center access must abide by the following rules:
• UA CatCards must be worn visibly at all times.
• Individuals must not touch equipment or supplies belonging to other departments.
• Access must not be used to allow any unauthorized person into the Data Center.
• An individual that has access MUST formally log in and out ALL visitors that are accompanying them into the Data Center.
• Individuals with access privilege must abide by all policies and procedures as described in the UITS Data Center Access Policies and Procedures document.
• Violating these rules can result in Data Center access being revoked and/or disciplinary action.
• Read and abide all Data Center access policies and procedures.

I fully understand and agree to these rules. I also agree to provide my full cooperation during any investigation concerning a security matter, which might have occurred in the Data Center during a time when my presence in the facility has been recorded.

Abuse of this access privilege and/or non-compliance with this agreement may result in removal of access and/or disciplinary action.

Applicant’s Signature: ___________________________ Date: ________________
Applicant’s Supervisor Name: _________________________________________________
Applicant’s Supervisor Signature: ___________________________ Date: ________________
Access Level: Unescorted Access □ Vendor Access □
IS Assistant Directors Signature: ___________________________ Date: ________________
Appendix B: Data Center Unescorted Access Request Procedure

1. Each employee requesting unescorted access to the Data Centers must complete a Data Center Access Agreement form.

2. The employee’s manager must sign the Access Agreement form before it can be submitted for review.

3. The ISOC Assistant Director will review all access requests. The applicant and their supervisor will be notified of the decision by email.

4. All submitted Data Center Access Agreement forms will be filed in the ISOC office.

5. The employee’s CatCard will then be authorized for access to the authorized Data Centers specified in the access request form.

6. If the Access Request form indicates an access request to more than one Data Center, the access requests will be evaluated and authorized separately.

7. An employee’s manager may appeal a denial of access via email to the ISOC Assistant Director. The email should include an expanded explanation for the employee access requirements. In the event that the denial is upheld, an appeal can be delivered, in writing, to the Infrastructure Services Senior Director. The decision of the Infrastructure Services Senior Director is final.
Appendix C: Data Center Etiquette

1. All work areas must be kept clean and free of debris. Staff performing work in the Data Centers must ensure that they have left the areas as clean as they were before beginning their work.

2. To reduce fire hazards rack enclosures must be kept neat and free of manuals, media, boxes and unused equipment. Rack enclosures are not storage cabinets and must only be used for functioning equipment.

3. Doors on all racks should remain closed at all times except during maintenance.

4. Cables should never be strung outside of rack enclosures. Cabling between rack enclosures of adjacent racks is accepted provided sufficient pass-through chassis are in place.

5. Under no circumstances should any customer:
   a. Lift floor tiles without prior knowledge, consent, and oversight of the ISOC staff.
   b. Tampering with or interfering with the normal function of the Transformers or Power Distribution Units (PDU).
   c. Tampering with or interfering with the normal function of the Air Conditioning units.
   d. Plugging any device into another cabinet’s power supply.
   e. Removing any cables or power connections from equipment other than those covered by your SLA.

6. The Data Center Manager should be contacted immediately if any customer requests access to the Data Center machine room infrastructure and/or environmental systems.

7. Under no circumstance should any food and beverages of any kind be within the raised floor area of Data Center. Food and beverages must only be consumed in the break room or the Operations Center. Beverages and other consumables many only be transported to and from the break room in spill proof containers.
Appendix D: Data Center Approved Vendor Access Procedure

Note: A Departmental Sponsored Visitor (DSV) ID must be obtained before a CatCard can be issued. The vendor must request a DSV from the UITS department sponsoring the vendor’s access to the Data Center. CatCard’s can be purchased at the CatCard office in the Student Union at a cost of $25/per card.

1. All members of a Vendor’s maintenance team granted unescorted access to the Data Center must display the University CatCard that was issued specifically for that individual. Sharing CatCards is strictly prohibited.

2. Each individual vendor requesting unescorted access to the Data Centers must complete the UITS Policies and Procedures Access agreement form. The form must be signed by the Assistant Director of the UITS department sponsoring the vendor.

3. The ISOC Assistant Director will evaluate and authorize the request if there is a legitimate business need. In the event that the request is denied, the vendor and sponsoring UITS department will be informed by email.

4. After approval of the access request, the access agreement form will be filed in the ISOC office and the Vendors CatCard will be authorized for swipe access.