

**BY ORDER OF THE COMMANDER  
SCOTT AIR FORCE BASE**

**SCOTT AIR FORCE BASE  
INSTRUCTION 33-100**

**3 MAY 2012**



***Communications and Information***

***MANAGEMENT OF THE SCOTT AFB  
DATA CENTER***

---

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available on the e-Publishing website at [www.e-publishing.af.mil](http://www.e-publishing.af.mil) for downloading or ordering.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: 375 CG/CCA

Certified by: 375 CG/CC  
(Col Patrick J. Gooley)

Pages: 11

---

This instruction implements Air Force Policy Directive 33-1, *Information Resources Management* and provides guidance on the management of the physical configuration of the Scott AFB data center. It provides shared management of the limited resources available in the facility. Its purpose is not to prevent the installation or changes to the facility, but to ensure that all equipment and systems meet standards that do not negatively impact other existing or planned systems. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afrims/afrims/>. Other Services, Agencies, and Commands will comply with their particular records disposition guidance. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication*, through the appropriate functional chain of command to the Commander, 375th Communications Group, 859 Buchanan Street, Scott AFB IL 62225-5101.

## **1. Overview.**

1.1. Background. Since the establishment of the Scott AFB data center, problems have arisen repeatedly related to facility safety, security, and installation practices. A variety of informal agreements temporarily resolved issues; but over time, problems would resurface. The purpose of this instruction is to codify the operations and maintenance (O&M) standards

for those using data centers managed by the 375th Communications Group (CG), and to provide a means to update and improve those rules over time.

1.2. Data centers functionally support those systems installed within the facilities. The basic design shall be simple, clean, modular, and most importantly, cost efficient. The policies and standards prescribed herein serve to provide the required functionalities, meeting the basic design criteria.

**2. Applicability.** This instruction applies to all organizations with equipment hosted by the Scott AFB data center.

2.1. Implementation of this guidance will be managed by the Data Center Configuration Control Review Board. The Board is responsible for centralized storage of records, coordination of plans, approvals of waivers, and dissemination of information related to the management of the facility. The Data Center Configuration Control Review Board Charter is established in [Attachment 3](#) of this instruction.

**3. General.**

3.1. All systems and equipment being installed into the data center will comply with this instruction. Equipment and cabinets that are already installed will only need to comply with safety and security policies until relocated or replaced. Upgrade of major components in a cabinet requires upgrade of the entire cabinet to meet the current standards described in this instruction. The Data Center Configuration Control Review Board shall make the determination if a requested change is deemed major or minor. It is the responsibility of the functional system managers to advise their project management offices (PMOs), contractors, and subcontractors of these standards.

3.2. The data center manager or facility electricians will apply power to new equipment only after that equipment has been inspected to the standards identified in [Attachment 1](#) of this instruction by the 375th Communications Squadron quality assurance office and installations specifically approved by the 375 CG Chief of Plans and Programs.

3.3. Exceptions to the policy described in this instruction will be considered on a case-by-case basis. Requests for exceptions to these policies and standards will be submitted by an O5 or civilian equivalent grade in writing to the Commander, 375 CG through the Chief, Plans and Programs (375 CG/SCX). The 375 CG/SCX will respond within 10 business days with a decision. Work will not start until the waiver has been formally approved. Noncompliant or unapproved starts will be immediately removed.

**4. Operations.**

4.1. Changes to existing physical configurations will be requested through the 375 CG Cyberspace Infrastructure Planning System (CIPS) application. Requests must include all the information listed in [paragraph 8](#) and below. These change requests will be forwarded to the Data Center Configuration Control Review Board for approval or disapproval.

4.2. All Authorized Service Interruptions (ASI) or any activity that may create a hazardous condition (HAZCON) for the facility shall be coordinated and approved NLT 30 days prior to execution. The data center manager will serve as the gatekeeper for such requests.

4.3. Each agency with equipment installed in the data center will provide Mission Assurance Category (MAC) (DoD Directive 8500.01E, *Information Assurance*) data to the data center

manager. The MAC data will be used to shut down systems during facility emergencies (See **paragraph 8.10**).

**Table 1. Mission Assurance Categories.**

<b>MAC I</b>	Hardware handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of MAC I hardware is unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I hardware requires the most stringent protection measures.
<b>MAC II</b>	Hardware handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II hardware requires additional safeguards beyond best practices to ensure assurance.
<b>MAC III</b>	Hardware handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

4.4. All electronic devices in cabinets will be labeled on the device face using Standard Forms 710, *Unclassified (Label)*, or 711, *Secret (Label)*, as appropriate. The labels should generally be placed in the upper left corner of the face of the device, but this may be adjusted if the design of the device face does not permit application of the label in that location.

4.5. Hot spares are considered to be part of an operational system. Cold spares will be kept off-site and brought to the facility only when required.

4.6. Equipment that is removed from service will be removed from the server floor as soon as possible. The server floor will not be used as storage pending disposition of discontinued Information Technology (IT) assets or as a placeholder for a future installation.

4.7. The data center has spaces designated for three services: operations, staging, and storage. The data center floor is the operations area and will be used only to house operational equipment. The staging area is the only area where materials may be removed from their shipping packages. Shipping and packing materials will not be brought into the server room. Due to space cleanliness considerations, equipment brought into the facility

should be assembled in the staging area and installed as quickly as is reasonably possible. The data center manager will assist program and system managers in scheduling use of this temporary build-up area normally not to exceed 5 business days. Storage cabinets are permitted only in the storage area. The server room will not be used to store materials, even on a temporary basis.

4.8. Cabinets on the server room floor will not be used for the storage of supplies, maintenance materials, tools, unmounted test equipment, or the like.

## 5. Facility Cleanliness.

5.1. Cleanliness of the data center is of primary importance. Dirt and trash present safety problems and are also likely to cause premature equipment failure. No trash will be permitted on the server floor. Continued issues with work area cleanliness can result in loss of facility access.

5.2. The cost to provide cleaning services to the server floor and the entire subfloor area will be borne by the users in accordance with Host Tenant Support Agreements.

5.3. Food and drinks are not permitted on the server floor.

5.4. A staging area has been created to allow personnel to uncrate equipment without bringing packing and shipping materials into the server room. Personnel using the staging area will remove all packing material and dispose of it outside of the facility. The staging area is not to be used for storage of equipment, tools, or other materials. Personnel using the area are responsible for security of their materials. The area will be used only for same-day delivery and setup, and will be cleaned by the using personnel at the end of each duty day.

## 6. Security.

6.1. Devices emitting radio frequency signals (i.e., pagers, personal digital assistants (PDAs), cell phones, Blackberries, etc.) are prohibited inside the facility. They must be left outside the building or may be temporarily stored in the secure electronic device locker located in the foyer near the main entrance to the facility. Secure mobility environment—portable electronic devices (SME-PEDs), in the sensitive compartmented information facility (SCIF) mode, are permitted.

6.2. Tapes and system media will not be stored on the server floor, regardless of the security classification of the server room or the media. All media will be marked in accordance with current security classification guidance.

### 6.3. Facility Access:

6.3.1. All personnel who require daily-unescorted access to the data center must submit AF Form 2586, *Unescorted Entry Authorization Certificate*, through their unit security manager to the 375 CG, Unit Security Manager, commercial (618) 256-4417, or DSN 576-4417. If approved, security forces will issue an AF Form 1199, *Controlled/Restricted Area Badge*.

6.3.2. Personnel requiring periodic access will submit a visitor access list (VAL) to 375 CG, Unit Security Manager. Visitors from other installations will submit a visitor access request (VAR) no less than 2 duty days before access is necessary to the 375 CG Security Manager through the Joint Personnel Adjudication System (JPAS) – security

management office (SMO) Code: SF1LFMV16. The security manager will forward the validated requests to the MAJCOM/Air Force Forces Communications Coordination Center (M/ACCC), who will issue temporary badges to the visitor(s).

6.3.3. Access to the facility is ONLY through the front (West) entrance. Other doors shall not be used to depart the facility except in the case of an emergency.

6.4. Possession of an AF Form 1199 with area 15 displayed DOES NOT automatically grant access to the entire facility. It provides access only to the main hallway. The data center manager will provide access to other areas based upon clearly defined need.

6.5. Only equipment listed on an approved Scott AFB CIPS request will be permitted into the facility. Prior to bringing equipment to the facility, or having equipment delivered to data center, call the data center manager to coordinate a delivery date/time. All equipment brought into data center will be brought in through the north loading dock door and checked by the data center manager. Equipment being brought in for emergency restoration after duty hours will be checked in through the M/ACCC.

6.6. Vehicle Access.

6.6.1. Vehicles requesting access through the gated area must be met at the sliding gate for verification of the need to enter.

6.6.2. All contractor vehicles requesting entry into the gated area will be inspected. The person providing access will do a cursory look inside the vehicle for any suspicious devices. Once completed that person will conduct a walk-around of the vehicle and use a hand-held mirror to inspect the under carriage of the vehicle.

6.6.3. During FPCON Charley or higher, vehicles will not be allowed to enter the gated area without the approval of the 375 CG/CC or his designee.

## 7. System Engineering.

7.1. Prior to ordering or purchasing new programs, the program advocate shall verify with base engineers that equipment can be added within the existing facility infrastructure capacity. If the addition of the new program results in required facility infrastructure upgrades (electrical and/or heating, ventilation, Air Conditioning (HVAC) expansions), then the cost to change the infrastructure to support the new start will be borne by the program, not by the facility.

7.2. Power load and heat generation are critical concerns in large data centers. New installations shall use technologies that consume less power and generate less heat. Virtualization is recommended. Whenever possible, engineers will select equipment with 208-volt input power.

7.3. The Installation Completion Checklist ([Attachment 2](#)) will be satisfactorily completed on all newly installed equipment BEFORE that system or equipment is placed into service.

7.4. Seismic protection for Zone 2 is required.

7.5. Installations shall comply with the Air Force Instructions, Air Force Occupational Safety and Health (AFOSH) standards, and the Air Force Technical Orders (T.O.) listed in [Attachment 1](#) as well as all other applicable engineering technical letters. The other

documents listed are provided for reference, and general compliance with those documents is strongly recommended.

7.6. Equipment cabinets shall be black in color with full side panels on each side. Panel blanks will be installed in all unused spaces in the cabinet. Cooling cabinet airflow will flow through the front of the cabinet, through the electronic device, into the cabinet interior, and out the top of the cabinet using a fan to maintain positive airflow. Cabinet installations shall include power strips that are compatible with the data center power management system—contact the data center manager for technical criteria.

7.7. Cabinets (temporary or permanent) will be sited only by the data center manager. Prior to the approval of the installation of any cabinet, the requesting installer will advise the data center manager of the cabinet weight to ensure that recommended floor loading is not exceeded.

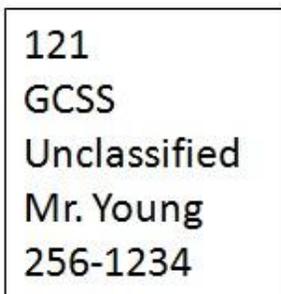
7.8. Floor penetrations shall be sized only large enough to facilitate the cable or conduit and its physical protection. Floor penetrations will be fire stopped in accordance with the National Electric Code, paragraph 300.21. The data center manager is responsible for making all floor penetrations. The program manager is responsible for the physical protection of the cable through the penetration (hole) and installation of the fire-stop.

7.9. The sub-floor area is used for the distribution of HVAC and this is considered a plenum. All cabling in the sub-floor area that is not in a metal duct or conduit must be plenum-rated in accordance with Article 800 of the National Electrical Code and National Fire Protection Standard 90A.

7.10. Equipment and cabling that are no longer required for operations shall not be abandoned in place. Obsolete equipment shall be removed in its entirety.

7.11. Program managers or other personnel installing equipment in cabinets will ensure that the front and the back of each equipment cabinet are marked in accordance with **Figures 1 and 2**. The front label will include cabinet number, program name, classification of processors, support point of contact, and point of contact phone number in at least size 28 font. The rear label will identify power distribution unit (PDU) or circuit breaker panel and the circuit breaker number(s) in at least bold size 40 font. These labels will not be hand-written and will be easily readable by any person standing in the aisle in front of the cabinet. The font size will be prominently visible for use in emergency power shutdowns.

**Figure 1. Cabinet Front Label.**



**Figure 2. Cabinet Rear Label.**

PDU	5
CB	9

7.12. System managers will ensure the data center manager is provided a rack elevation diagram for each cabinet in PowerPoint or Visio format. The data center manager will maintain these documents for use by the Data Center Configuration Control Review Board.

## **8. Data Center Management.**

8.1. The data center manager will maintain a floor plan reflecting current and planned equipment locations. The data center manager will assign space for future expansion and equipment installers will comply with his/her assignments.

8.2. The data center manager will develop a long-range plan for the management and assignment of power and HVAC load and brief this plan to the Data Center Configuration Control Review Board and the 375 CG Commander annually.

8.3. Subfloors will be cleaned in accordance with AFOSHSTD 91-64, *Data Processing Facilities*, paragraph 2.4.

8.4. The data center manager will build an Equipment Designator Database (EDD) listing the electrical consumption, heat load presented, cabinet and equipment weight, and the rack space used by each device in each cabinet. Reports will be generated listing load by cabinet, load by power panel, load by room, cumulative load to the facility, and weight per square-foot of each cabinet. The database will reflect each piece of equipment brought into and out of the facility and include those used in administrative areas. The data center manager will maintain schematics of electrical services supporting IT in the facility and rack elevations (face equipment diagrams) of each cabinet.

8.5. The data center manager will publish and maintain plans and procedures for prioritizing and implementing the shedding and restoration of electrical load should problems with the air conditioning or electrical services occur.

8.6. The data center manager will ensure each power distribution cabinet and each circuit breaker panel has an accurate panel schedule showing, at a minimum, all cabinets powered by that panel or power distribution unit circuit.

8.7. In the event of a loss of power or HVAC to the facility, the data center manager and supporting staff will implement the shutdown guidance provided by the 375 CG Chief of Plans and Programs and approved by the 375 CG Commander. Equipment will be shut down in MAC order (least critical to most critical) when directed and approved by the Air Mobility Command (AMC)/A6. This data will be reflected in the load-shed plan, used during emergencies.

MICHAEL J. HORNITSCHKEK, Colonel, USAF  
Commander

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

- AF Instruction 32-1062, *Electrical Power Plants and Generators*, 1 June 2005
- AF Instruction 32-1063, *Electrical Power Systems*, 10 June 2005
- AF Instruction 32-1064, *Electrical Safe Practices*, 25 May 2006
- AFOOSH Standard 91-64, *Air Force Occupational Safety and Health Standard for Data Processing Facilities*, 1 August 1997
- AFSSI 7702, *Emission Security Countermeasures Reviews*, 30 January 2010
- T.O. 31-10-2, *Air Force Communications Command (E-I Standard) – Standard Installation Practices, Fanning and Forming Conductors For Ground Comm-Electronic Equipment*, 15 August 1977
- T.O. 31-10-10, *Air Force Communications Command (E-I Standard) – Standard Installation Practices, Anchoring Devices For Ground Comm-Electronic Equipment*, 1 March 1973
- T.O. 31-10-24, *Air Force Communications Command (E-I Standard) – Standard Installation Practices – Comm Sys Grounding, Bonding, and Shielding*, 15 November 2011
- T.O. 31-10-27, *Air Force Communications Command (E-I Standard) – Standard Installation Practices Equipment Designations*, 1 June 1973
- T.O. 31-10-29, *Air Force Communications Command (E-I Standard) – Standard Installation Practices Erection and Assembly of CEM Equipment*, 10 May 1968
- T.O. 31-10-34, *Air Force Communications Command (E-I Standard) – Standard Installation Practices – Fiber Optic Communications Cables and Connectors*, 1 October 1998
- BICSI Data Center Design and Best Practices, 002-2011, 15 March 2011
- BICSI Network Design Reference Manual, 7th Edition, (No Date)
- BICSI Telecommunications Distribution Methods Manual, 12th edition, (No date)
- ANSI/TIA/EIA TSB-67, *Transmission Performance Specifications for Field Testing of Twisted Pair Cabling*, October 1995
- ANSI/TIA/EIA-526, *Standard Test Procedure for Fiber Optic Fibers, Cables, Transducers, Sensors, Connecting and Terminating Devices, and Other Fiber Optic Components*, September 1992
- ANSI/TIA/EIA-568-B, *Commercial Building Wiring Standard*, May 2001
- ANSI/TIA/EIA-607, *Telecommunications Bonding and Grounding Standard*, August 1994
- ANSI/TIA/EIA-942, *Telecommunications Infrastructure Standard for Data Centers*, April 2005
- GR-63-CORE, *Issue 3 NEBS™ Requirements: Physical Protection*, March 2006
- DISA Circular 310-55-9, *Base Level Support for the Defense Information System Network (DISN)*, 5 November 1999

MIL-HDBK-232A, *Red-Black Engineering/Installation Guidelines*, 24 October 2000

MIL-HDBK-419A, *Military Handbook of Grounding, Bonding, and Shielding of Electronic Equipment and Facilities*, 29 December 1987

MIL-STD-1542B, *Electromagnetic Compatibility and Grounding Requirements for Space System Facilities*, 15 November 1991

NFPA 70, *National Electric Code*, 2012 Edition

NFPA 13, *Standard for the Installation of Sprinkler Systems*, 2010 Edition

NFPA 72, *National Fire Alarm Code*, 2010 Edition

NSTISSAM TEMPEST/2-95, *National Security Telecommunications and Information Systems Security Advisory Memorandum TEMPEST/2-95*, 12 December 1995

UFC 3-560-01, *Electrical Safety, O&M*, 6 December 2006

### ***Prescribed Forms***

None

### ***Adopted Forms***

AF Form 1199, *Controlled/Restricted Area Badge*, 1 November 1986

AF Form 2586, *Unescorted Entry Authorization Certificate*, 1 November 1998

Standard Form 710, *Unclassified (Label)*, 1 January 1987

### ***Abbreviations and Acronyms***

**AFOSHS**—Air Force Occupational Safety and Health Standards (AFOSHSTD)

**AMC**—Air Mobility Command

**ANSI**—American National Standards Institute

**BICSI**—Building Industry Consulting Standards Institute

**CG**—Communications Group

**CIPS**—Cyberspace Infrastructure Planning System

**HAZCON**—Hazardous Condition

**HVAC**—Heating, Ventilation, Air Conditioning

**IT**—Information Technology

**MAC**—Mission Assurance Category

**M/ACCC**—Major Command/Air Force Forces Communications Coordination Center

**NEC**—National Electrical Code

**NFPA**—United States National Fire Protection Association

**TIA/EIA**—Telecommunications Industry Association/Electronic Industries

**T.O.** —Technical Order

**Attachment 2****INSTALLATION COMPLETION CHECKLIST**

1. Is the configuration of the cabinet and equipment built to the specifications described in the technical solution of the approved CIPS? (Paragraph 4.1.)
2. Is each electronic device in the cabinet marked with a SFs 710 or 711? (Paragraph 4.4.)
3. Have cold spares been removed from the cabinet? (Paragraph 4.5.)
4. Has all trash been removed from the facility? (Paragraph 5.1.)
5. Have all installation material residue been removed from the facility? (Paragraph 4.7.)
6. Have all tapes and electronic media been removed from the cabinet and surrounding work area? (Paragraph 6.2.)
7. Does the installation comply with Air Force Instructions and Air Force Technical Orders? (Paragraph 7.5. – This requires documentation per Paragraph 3.2.)
8. Does the installation (cabinet) meet the requirements prescribed for zone 2 seismic protection? (Paragraph 7.4.)
9. Is the equipment cabinet black? If not, has a waiver been approved by the Data Center CCRB? (Paragraph 7.6.)
10. Was the cabinet sited by the data center manager, and documented on the facility floor plan? (Paragraph 8.1.)
11. If this is a replacement or upgrade, was all unused wiring removed? (Paragraph 7.9.)
12. Is the cabinet front and rear properly marked? (Paragraph 7.10.)
13. Is the data associated with the cabinet equipment entered into the Equipment Designator Database? (Paragraph 8.4.)
14. Is the equipment in the cabinet documented in the facility load shed plan? (Paragraph 8.7.)
15. Have rack elevations been updated? (Paragraph 7.11.)

### Attachment 3

#### DATA CENTER CONFIGURATION CONTROL REVIEW BOARD CHARTER

- 1. Purpose.** The Data Center Configuration Control Review Board provides oversight and management of equipment siting, electrical and HVAC load. The overall purpose of each review is to ensure installed systems and equipment do not exceed facility capacity
- 2. Background.** Demands for space in the Scott AFB data center continue to exceed available capacity of the facility. Previous incidents of excessive load jeopardized the ability of HVAC and generators to carry the load in HAZCON situations. An operational review board recommended establishing the Data Center Configuration Control Board.
- 3. Scope.** The Board will oversee implementation of this guidance and direct changes as necessary. The Board is responsible for coordination of plans, approval of waivers, and dissemination of information related to the management of the facility. The Board will review and approve/disapprove change requests at least bi-monthly. Technical considerations related to the HVAC and electrical load will be addressed, and change requests approved/disapproved by the board.
- 4. Team composition.** The Data Center Configuration Control Review Board is comprised technical representatives from:
  - 4.1. VOTING MEMBERS:
    - 4.1.1. The 375 CG [Chair].
    - 4.1.2. United States Transportation Command (USTRANSCOM) J6.
    - 4.1.3. Army Surface Deployment and Distribution Command (SDDC) G6.
    - 4.1.4. AMC A6.
    - 4.1.5. Eighteenth Air Force (18 AF) A6.
    - 4.1.6. Air Force Network Integration Center (AFNIC) EA.
    - 4.1.7. The 375th Civil Engineer Squadron.
  - 4.2. ADVISORY MEMBERS:
    - 4.2.1. The 375 CG/SCX.
    - 4.2.2. The 375th Computer Support Squadron (CSPTS).
    - 4.2.3. The 375 CS.
    - 4.2.4. Detachment 3, 561st Network Operations Squadron (NOS).
- 5. Membership Roles.**
  - 5.1. Voting members review requests for changes, justifications, and approve or recommend strategies to reduce load.
  - 5.2. Representation by the chair and four voting members shall be considered a quorum.
  - 5.3. A simple majority of all voting members shall be used to determine if issues presented to the board pass or fail. In the event of a tie vote, the chair shall determine whether the issue passes, fails, or is tabled for further study.
- 6. Upon approval of the attached Scott AFB instruction, this Charter will be considered approved.**