



Australian
National
University

AUSTRALIAN NATIONAL UNIVERSITY DATA CENTRE STANDARDS

ANU ITS Data Centre Operations

Version: 1.1
Date: 18th March 2014
Status: Final
Type: Internal
Prepared By: David Hardwicke and Geoff Barlow

Document Change Control

Version	Authors	Summary of Changes
V0.1	David Hardwicke	Original Document
V0.2	David Hardwicke Geoff Barlow David Richardson	Move from multiple documents to one generic standards document covering all data centres Formatting changes
V0.3	David Hardwicke Geoff Barlow David Richardson	Change to generic ICT staff references Name change from 'ICT Facilities Staff' to 'Data Centre Operations Staff' Formatting changes
V0.4	David Hardwicke Geoff Barlow David Richardson	Removal of 'Network Environments' from name Changed Responsible Officer throughout sections 1-3 to include Associate Director – Infrastructure Updated equipment installation and removal procedures detailed in section 3.3, in particular sections 3.3.1 – notification, 3.3.2 – racks and equipment layout, 3.3.7 – completion of works Updated section 4, providing more detail on data centre security Added appendix 3 -Patch Lead Colour Standard
V0.5	David Richardson	Slight wording changes
V1.0		Final document for publication
V1.1	David Hardwicke Geoff Barlow	Included NCI delegate approval of access for NCI data centre in section 4.1 Principles for access details moved from section 4 to section 1 Change to section 4.2 item 9 – contractors will be required to undergo induction with DOCS Included non-standards communication cables under section 4.3.3 item 9

Related Documentation

[ANU Data Centre Request for Work](#)

[ANU Data Centre Request for Access](#)

Table of Contents

1 Executive Summary.....4

2 Data Centre Operations Staff Role4

3 Security5

4 Data Centre Access and Behaviour.....5

 4.1 Conditions of Admittance5

 4.2 Data Centre Behaviour6

 4.3 Equipment Installation and Removal8

 4.3.1 Notification8

 4.3.2 Racks and Equipment Layout.....8

 4.3.3 Communications Patching9

 4.3.4 Power10

 4.3.5 Cooling10

 4.3.6 Faults.....11

 4.3.7 Completion of Works11

5 Facilities Audit and Change Management11

Appendix 1 : Rubbish Handling12

Appendix 2 : ANU Data Centre Power and Cooling Infrastructure.....13

 Power13

 Leonard Huxley Data Centre13

 Crisp Data Centre13

 NCI Data Centre13

 Cooling13

 Leonard Huxley Data Centre13

 Crisp Data Centre13

 NCI Data Centre13

Appendix 3 : Patch Lead Colour Standard14

1 Executive Summary

This document outlines the standards that are enforced within the data centres at the Australian National University. It details the responsibilities of data centre users and those of Data Centre Operations Staff, with the purpose of making you aware of what is expected of you when working in an ANU data centre. This document must be referenced by all users prior to entering any of the ANU's data centres. Non-complying data centre users will have their access revoked at the discretion of the Data Centre Operations Manager and/or the Associate Director, Infrastructure.

The principles underlying access to and use of the data centres are:

- Safety is paramount. All activity must be conducted in a manner that ensures a safe working environment is maintained at all times.
- Security of physical infrastructure is critical for the University's business continuity and for the security of the University's information and information systems.
- Physical access is minimised and granted on a justifiable needs basis.
- The data centre facilities are managed as a whole. Any activity in one part of the room may affect the conditions in other parts of the room. Consequently, a single facilities management strategy applies and is implemented by DCOS.
- All changes within the data centres must be approved and documented via the ANU IT Change Management process.

2 Data Centre Operations Staff Role

The University Officer responsible for the ANU data centre facilities is the Associate Director, Infrastructure, and via delegation, Data Centre Operations Manager. Data Centre Operations Staff (DCOS) are responsible for the day-to-day management of the facility. DCOS are responsible for the following tasks.

1. Provide, install and manage facilities and support services for the IT equipment in the data centres, including but not limited to power distribution, cooling, optical fibre and UTP communications cabling, and cable management infrastructure.
2. Provide sustainable asset management of the data centres and their facilities, including the design and implementation of facilities life extension and development.
3. Install and remove all IT equipment in the data centres, unless an alternative arrangement is reached.
4. Manage physical access.
5. Ensure data centre users adhere to procedures and standards specified in this document.

3 Security

Physical security is of utmost importance in the ANU data centres. Biometric fingerprint readers, as well as CARDAX proximity readers are installed on entrance doors to control access into the data centre. These readers also provide auditing capabilities and are monitored by DCOS and by ANU security. CCTV cameras are also utilised within all ANU data centres providing surveillance coverage of data centre entrance and exit doors, as well as other key zones within the data centres. Signage is deployed ensuring all who enter are aware of the surveillance in progress.

In addition to the abovementioned security measures, all data centre users must remain mindful of physical security at all times. This includes adhering to the following:

1. Ensure all building and data centre perimeter doors are closed securely after entering and leaving a data centre
2. Ensure that they are not 'tailgated' as they enter a data centre.
3. Under no circumstances grant access to an individual who claims to have lost or forgotten their access card.
4. Report any suspicious activity to a member of DCOS and/or ANU Security on 61252249, as appropriate.
5. Notify a member of DCOS and/or ANU Security of any breach of security in an ANU data centre.

4 Data Centre Access and Behaviour

4.1 Conditions of Admittance

Physical access by individuals into the data centres is based on a current, identified need which has been approved by the Delegated Authority – Associate Director, Infrastructure and/or Data Centre Operations Manager. Access to the NCI data centre must also be approved by the NCI Delegate.

Individuals who require ongoing access to an ANU data centre should first seek endorsement from their supervisor, identifying a legitimate need for access, before submitting an application for access. This application must be by way of a submitting a completed 'ANU Data Centre Request for Access' form, to the Delegated Authority.

Once approved by the Delegated Authority, new users will be required to undergo an induction session with a DCOS member, before being permitted to access any ANU data centre unaccompanied. Having undergone an induction session for the relevant data centres, users will have their fingerprints authorised and will be given CARDAX access to the necessary doors.

DCOS will de-authorise access according to the timeframe specified in the 'ANU Data Centre Request for Access' form. DCOS will also undertake 3 monthly access audits and users with extended period of non-use will be requested to provide revalidation of their ongoing need for access.

4.2 Data Centre Behaviour

The ANU data centres are utilised by many groups and all users must be considerate of other parties in the room. Once users have been granted access to the data centre, they must adhere to the following requirements and obligations:

1. No food or drink is permitted in the data centres.
2. The data centres are to be kept tidy and safe at all times. This involves adhering to the following:
 - a. Any work requires a safe workplace to be maintained, any hazards to be identified and made safe, working parties to be made conscious of hazards and appropriately skilled and aware, and the work area to be returned to normal conditions on completion of the work.
 - b. All data centre users should exercise caution in the data centre when works are in progress, to avoid missing floor tiles, obstacles and other hazards.
 - c. Protect your feet. Ensure your footwear is appropriate for the activity you are undertaking in the data centre.
 - d. Protect your ears. The data centres are noisy environments and includes high noise spots. Hearing protection is a requirement for extended exposure to the noise. Earmuffs and disposable earplugs are available for use, located on the shelving inside the data centres.
 - e. Protect your eyes. The lasers associated with optical fibre communication systems in the data centres present an eye safety risk. Exposure can cause irreversible eye damage. Adhere to all warnings on devices and exercise caution when working with lasers.
 - f. Data centre users are not to access the sub floor. If access is required for a specific reason, users must ask a member of DCOS for assistance.
 - g. Data centre users are not to climb onto racks. If a data centre user has a requirement to access the top of a rack, they must seek assistance from a member of DCOS.
 - h. Do not leave rubbish on the floor in the data centre. Whenever possible, items should be unpacked prior to entry into the data centre. All rubbish, packing materials or unwanted parts are to be removed from the data centre as soon as possible. Details on how different types of rubbish should be handled for each data centre, is included in Appendix 1.
 - i. Trolleys and crash carts are available for use by data centre users. These items are to be freed up and returned on the completion of work, or the end of the day (whichever is sooner), unless prior approval is given by DCOS.
 - j. Return all borrowed tools when work is finished or at the end of the day (whichever is sooner). Tools are not to be removed from the data centre.
 - k. Equipment such as temporary leads, monitors, laptops etc. are not to be left on the data centre floor for longer than required for the job at hand, and certainly not overnight, unless prior approval is given by DCOS
 - l. No loose items, such as packaging, parts or leads are to be stored in racks.
 - m. Rack doors are to be secured following work or during times when the rack is unattended for extended periods. Racks are to remain unlocked except RackTek racks which have their keys left in the doors.
 - n. Storage cupboard doors are to remain closed when not in use.
 - o. Spare cage nuts, bolts, caps, ties, etc., are to be placed in the appropriate containers on the shelves inside the data centre. Any damaged parts (damaged threads etc.) should be disposed of. Users must inform DCOS of damage to larger items within the data centres,

3. Data centre users are not to enter data centre plant rooms unless authorised by DCOS.
4. Portable telephones are located in the data centres, available for users as required.
5. GPOs are available around the data centres for laptops and other temporary equipment usage. These outlets are not UPS or generator backed.
6. Visitors must be escorted by an authorised data centre user at all times. Data centre users are under no circumstances to loan their access cards to visitors.

7. Data centre tours

- a. A member of DCOS should be notified of tours at least 5 working days in advance. More notice is preferable as work restricting safe access to the data centre, or presenting other safety hazards, may be scheduled.
- b. Tours will only be allowed with an accompanying data centre user. That user will be responsible for the behaviour of the people on the tour and for containing the group in the relevant area of the data centre.
- c. Any work areas or safety hazards will be identified and access restricted as appropriate.

8. Loading dock

Data centre loading docks are used frequently for equipment deliveries and dispatches. To ensure uninhibited access, vehicles must only be left in the loading dock areas while loading or unloading equipment. Where relevant, the safety chain or rails protecting the loading dock must be returned to position immediately following a delivery.

9. Contractor induction

Before leaving any contractor in the data centre, data centre users are responsible for ensuring that the contractor has undergone an induction with a member of DCOS. In addition to this, users should ensure that contractors are:

- a. Issued with an appropriate contractor access card to enable them to exit the data centre. Contractor cards are available for loan from DCOS.
- b. Issued with a parking permit if required, which are available for loan from DCOS. Under no circumstances are visitors to park in the loading dock areas unless loading or unloading their vehicle.
- c. Made aware of building security, especially automatic door locking times.

4.3 Equipment Installation and Removal

DCOS are responsible for the installation of all equipment in ANU data centres, unless an alternative arrangement is reached. Users who require work to be performed in an ANU data centre must lodge a request via the [ANU IT Service Desk](#), as detailed in section 4.3.1 below.

Data centre users and/or equipment manufacturer representatives, are responsible for the installation of parts in existing devices. When such work requires the reconfiguration of any physical aspect of a rack (power or communications requirements for example, the relevant parties are required to engage a DCOS member by lodging a request via the [ANU IT Service Desk](#), before proceeding with any work.

The following section details the responsibilities of data centre users when planning for and carrying out any work in an ANU data centre.

4.3.1 Notification

All requests for work within an ANU data centre must be lodged via the [ANU IT Service Desk](#). This process will require the completion of an “ANU Data Centre Request for Work” form to ensure that DCOS are provided with all the information necessary for carrying out the work. Service requests will carry a minimum completion time of 5 working days; however certain works may require the purchase of infrastructure with lead times of up to several months. Users should therefore ensure that service requests are lodged as soon as is possible when planning for work in an ANU data centre.

4.3.2 Racks and Equipment Layout

All new equipment must be rack-mountable and will be installed in the standard racks utilised within the ANU data centres. All racks are 42RU in height, have a width of 600mm or 750mm, and a depth of 1070mm or 1200mm, depending on the data centre. These racks will be fitted with power distribution units (PDUs), cable management strips, UTP patch panels, fibre optic break out trays (FOBOTS), and network management switches as required. The layout of this infrastructure will vary rack by rack and will be configured based on the specific requirements of the devices installed in that rack. The specific location of new equipment will be chosen by DCOS, through consultation with the relevant data centre users.

In instances where approval has been given for data centre users to install equipment in racks, the following points must be adhered to:

1. Equipment must be installed on RU boundaries.
2. Equipment should be installed beginning at the bottom RU.
3. No equipment is to encroach into the area at the top of the rack in front of preinstalled cabling infrastructure.

All tools, parts and cables required for work in the data centres are located on the shelving within the data centres. All tools and unused parts and cables are to be returned to the relevant location on completion of work or at the end of the day (whichever is sooner).

4.3.3 Communications Patching

DCOS will fit out racks with UTP patch strips and FOBOTs sufficient to meet the expected long-term requirements for each rack. Data centre users are responsible for the connection of all communications cabling to support their equipment in the ANU data centres. When carrying out this work, users must follow the guidelines detailed below. If difficulty is experienced with patching for any reason, or you are unable to comply with these guidelines, you should notify a member of DCOS who will provide assistance, or find a resolution as appropriate.

1. Use the shortest patch lead practical for the job.
2. Patch leads must be routed through horizontal and vertical cable tidies as appropriate. UTP and fibre have separate horizontal cable tidies.
3. No patch leads are to be run between racks without approval from DCOS.
4. No patch leads are to be run in the sub floor areas.
5. No UTP or fibre patch leads other than those supplied in the data centre are to be used in the data centre.
6. UTP and fibre patch leads colours should be selected in accordance with the cable standard detailed in Appendix 3.
7. Patch leads are to be run neatly, maintaining manageable densities in both horizontal and vertical cable tidies. In general, this will be achieved by evenly splitting patch cables from patch strips and FOBOTS to the left and right into the vertical cable tidies. Out of a FOBOT for example, fly leads should be routed as follows:
 - Cores 1-12 should be routed to the left.
 - Cores 13-24 should be routed to the right.
8. All spare fibre and UTP patch leads are to be capped before being returned to the appropriate container on the shelves within the data centre. Caps and twist ties required for this work are available on the shelving with the data centres.
9. In instances where a user has a requirement for high densities of cables such as InfiniBand or SAS within a rack or for this type of cable to run between racks, this must be discussed with a member of DCOS before proceeding.

4.3.4 Power

DCOS are responsible for connecting power to all equipment in ANU data centres, unless an alternative arrangement is reached between data centre users and DCOS. Electrical power in the ANU data centres is backed by a combination of UPS battery backup and diesel generators. Multiple UPSs are employed to support essential data centre load in the event of a power failure. In order for the UPS backup to be effective, it is important that the data centre load is balanced at the rack level. Most racks utilise two power distribution units (PDUs), each powered by a different source. All PDUs are remotely monitored by DCOS, who receive notifications when predefined thresholds are breached. The successful operation of this system is dependent on the following criteria being met.

1. The front panel of UPSs are to be used only by DCOS.
2. No power is to be run from sub floor areas except by DCOS.
3. Data centre users are not to access distribution boards or power distribution units.
4. No extension leads or power boards are to be used in racks or in sub floor areas.
5. PDU's are not to be removed from or installed in racks except by DCOS.
6. Users will not have access to any remote switching function on PDUs.
7. In the case of redundantly powered devices, power leads must be split, one into each of the two PDUs in the rack. These leads must not cross between banks on PDUs. That is, power leads from one device will be into bank 1 on both PDUs, or bank 2 on both PDUs.
8. The shortest power lead practical is to be used for the job.
9. Power leads are to be routed through vertical cable tidies as appropriate.

More specific detail on the power systems employed in the ANU data centres can be found in Appendix 2.

4.3.5 Cooling

DCOS are responsible for the implementation and management of the air conditioning strategies within the ANU data centres. Data centre environmental conditions and heat load distribution is remotely monitored and changes made as appropriate by DCOS. The cooling strategies employed vary between the ANU data centres and their effective operation is dependent on the following criteria being met.

1. The front panels of in-row cooling units are to be used only by DCOS.
2. Rack doors must be secured on completion of work or end of the day (whichever is sooner).
3. The doors into contained hot aisles are not to be left open at **ANY** time.
4. Blank off panels will be installed at the front of racks where appropriate, to prevent hot/cold air contamination. Data centre users are not to add or remove any such blanking panels before consulting a DCOS member.
5. In instances where sub floor cooling is utilised, DCOS will install appropriate floor tiles and vents to provide appropriate cooling of equipment. Data centre users are not to add, remove or change the configuration of these tiles or vents.
6. In certain instances, distribution of high heat load equipment across several racks may be necessary to achieve acceptable rack heat densities.
7. Data centre users are not to remove the ceiling panels of contained hot aisles, unless specific permission is granted by a member of DCOS.

More specific detail on the cooling systems employed in the ANU data centres can be found in Appendix 2.

4.3.6 Faults

Faults within the data centre should be handled in the following way.

1. If a user believes there is a fault with any item of data centre infrastructure, they should report it via the [ANU IT Service Desk](#). Users should not attempt to rectify faults themselves.
2. Any faults arising from work in a data centre should be reported to DCOS and via the [ANU IT Service Desk](#).
3. Faults identified out of business hours should be reported to ANU Security on 61252249, who will in turn notify the relevant parties.

4.3.7 Completion of Works

Following the completion of work performed in an ANU data centre, users must notify a member of DCOS, who will ensure the work complies with these standards. If the work complies with these standards, the DCOS staff member will update the service request ticket with their approval so that it can be closed.

5 Facilities Audit and Change Management

DCOS monitor the facilities in the ANU data centres and are continually reviewing the distribution of heat and power loads within the data hall. On occasion, it may be necessary to upgrade, replace or rearrange facilities to maintain the whole-of-room environment. Change requirements will be discussed with all relevant data centre users and plans developed to effect the required changes with minimal service impact.

Appendix 1 : Rubbish Handling

Table 1 - Rubbish Handling

Material Type	Disposal Method		
	Leonard Huxley Data Centre	Crisp Data Centre	NCI Data Centre
Recyclable plastic	Place in recycling bin on level 3 patio area.	Place in recycling station to NW of data centre.	Place in recycling bin located at the NW corner of the building.
Non-Recyclable plastic and foam	Place in hopper on level 2 loading dock. The rubbish bins in the data hall are for small items only.	Place in trade waste bins to NW of data centre. The rubbish bin in the data hall is for small items only.	Place in appropriate box against west wall of data hall. The rubbish bins in the data hall are for small items only.
Paper	Place in paper recycling bin in level 2 corridor.	Place in recycling station to NW of data centre.	Place in appropriate box against west wall of data hall.
Cardboard	Place in cardboard recycling station outside either Nuclear Physics or Earth Sciences. Small items may be placed in box on west wall of data hall.	Place in recycling station to NW of data centre.	Place in appropriate box against west wall of data hall.
Metal (including old and damaged UTP and power leads)	Place in marked box on west wall of data hall.	Place in recycling station to NW of data centre.	Place in appropriate box against west wall of data hall.

Appendix 2 : ANU Data Centre Power and Cooling Infrastructure

Power

Leonard Huxley Data Centre

The Leonard Huxley Data Centre utilises a combination of UPS and auto-start generator-backed power, to support essential data centre load in the event of a power failure. Mains power is also utilised within the data hall to support some non-essential loads.

Crisp Data Centre

Power in the Crisp Data Centre is UPS backed, providing approximately 10 minutes of runtime in the event of a power failure. The data centre has generator input capability but does not have an auto-start generator on site. In the event of a sustained power outage of greater than 10 minutes, power to the data centre will be lost.

NCI Data Centre

The NCI Data Centre utilises a combination of UPS and auto-start generator-backed power, to support essential data centre load in the event of a power failure. Mains power is also utilised within the data hall to support some non-essential loads.

Cooling

Leonard Huxley Data Centre

The Leonard Huxley Data Centre utilises multiple cooling technologies. Parts of the data centre employ hot aisle containment cooling technology, which utilises in-row cooling units that draw hot air from the contained hot aisle, and eject 24°C air into the data centre at the front of racks. Other areas of the Leonard Huxley Data Centre utilise HVAC units which provide cool air to the front of racks, through vents, via a sub floor plenum.

Crisp Data Centre

The Crisp Data Centre employs hot aisle containment cooling technology, which utilises in-row cooling units that draw hot air from the contained hot aisle, and eject 24°C air into the data centre at the front of racks.

NCI Data Centre

The NCI Data Centre employs hot aisle containment cooling technology, which utilises in-row cooling units that draw hot air from the contained hot aisle, and eject 24°C air into the data centre at the front of racks.

Appendix 3 : UTP and Optical Fibre Patch Lead Colour Standard

All fibre and UTP patch leads used in the ANU data centres are to follow the colour scheme below.

UTP



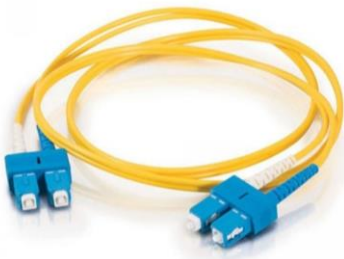
Yellow UTP patch leads are used for critical monitoring of the power and cooling infrastructure in the data centres. Patch leads of these colours are to be installed and removed by DCOS only.



Blue UTP patch leads are used for all other UTP connections in the data centre.

No colours other than those specified above are to be used in the data centres. If a user has a particular requirement to utilise an alternative colour patch lead, they must first seek approval from a member of DCOS.

Fibre



All Single mode (SM) fibre patch leads in the ANU data centres are yellow in colour. In general, SM fibre is used for long range links external to the data centres.



Multimode (MM) fibres within the data centres are orange, aqua, or salmon in colour. Any of these three colours can be used within the ANU data centres for MM installations. If a user has a reason to use a colour other than these in the data centre, they must first seek approval from a member of DCOS.