Crisp Data Centre Standards
11 November 2008

This document outlines the standards that are enforced within the Crisp Data Centre, and as amended from time to time. Also specified are the responsibilities of data centre users and those of data centre Facilities Management Staff. The effective operation of the specialised infrastructure solution supporting the Crisp Data Centre is dependent on strict adherence to the standards outlined in this document. These standards should be referenced by users prior to entering the Crisp Data Centre.

1 Facilities Management Staff Role
The University Officer responsible for the Crisp Data Centre facility is Head, Networks and Communications. The Head, Networks and Communications has identified Facilities Management Staff (FMS) who, in part, are responsible for the day-to-day management of the facility.

The FMS members for the Crisp Data Centre are:

Geoff Barlow: 53745  Dave Hardwicke: 58397  Kylie Paintain: 55034

FMS are responsible for the following tasks.

1. Provide rack unit (RU) space to users for the installation of computer equipment.
2. Provide, install and manage facilities and support services for the computer equipment in the data centre.
3. Provide sustainable asset management of the data centre and its facilities, including the design and implementation of facilities life extension and development.
4. Manage physical access.
5. Ensure data centre users adhere to procedures and standards specified in this document.

1.1 Equipment Provided
FMS will provide data centre users with RU space within 42RU APC SX data racks. These will be fitted with power distribution units (PDUs), cable tidies, UTP patch panels, fibre optic break out trays (FOBOTS), and network management switches. The exact layout of this infrastructure will depend on the specific requirements of the user and should be discussed with FMS prior to commencing work. Table 1 details some common rack layouts.
Table 1 - Rack Communications Layout

<table>
<thead>
<tr>
<th>RU Number</th>
<th>1F, 1U</th>
<th>2F, 1U</th>
<th>3F, 1U</th>
<th>1F, 2U</th>
<th>1F, 3U</th>
<th>4F</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>41</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>40</td>
<td>U</td>
<td>T</td>
<td>T</td>
<td>U</td>
<td>U</td>
<td>T</td>
</tr>
<tr>
<td>39</td>
<td>T</td>
<td>U</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>38</td>
<td>MS</td>
<td>T</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>F</td>
</tr>
<tr>
<td>37</td>
<td>T</td>
<td>MS</td>
<td>T</td>
<td>MS</td>
<td>U</td>
<td>MS</td>
</tr>
<tr>
<td>36</td>
<td>T</td>
<td>MS</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>35</td>
<td>T</td>
<td>MS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Where;
F denotes a single RU 24 core SC FOBOT
T denotes a single RU horizontal cable tidy
U denotes a single RU 24 port cat5e UTP patch strip;
MS denotes a single RU 48 port network management switch

Other equipment can be supplied and installed by FMS if required including:

1. Rack LCD monitor keyboard mouse
2. KVM switches
3. Rack shelves

*To see examples of racks in the data centre, or to discuss specific rack requirements, please contact FMS.*

2 Data Centre Access and Behaviour

2.1 Conditions of Admittance

Physical access by individuals into the data centre is based on a current, identified need which has been approved by the Delegated Authority – Head, Networks and Communications.

Individuals who require ongoing access to the data centre door should first seek endorsement from their supervisor, identifying a legitimate need for ongoing access. Once endorsed by the supervisor an application for ongoing access can be made to FMS. Once approved by Head, Networks and Communications, users will be given CARDAX access to the necessary doors.

When the ongoing access need is no longer required users should inform FMS to remove their access.

FMS will undertake periodic access audits and may request revalidation of the ongoing need for access. Any extended non-use will result in that access being
terminated (after confirmation by FMS from the user that access is no longer required).

2.2 Data Centre Behaviour

The data centre is utilised by many groups and users must be considerate of other parties in the room. Once users have been granted access to the data centre, the following conditions must be met.

The principles underlying the use and access to the data centre are:

- Safety is paramount. All activity requires a safe access environment to be maintained.
- 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 will affect the conditions in every other part of the room. Consequently, a single facilities management strategy applies.

Individuals entering the data centre must adhere to the following requirements and obligations:

1. No food or drink is permitted in the data centre.

2. The data centre is to be kept tidy and safe at all times. This involves adhering to the following:
   a. Any work requires a workplace safety plan to be in place, a safe workplace to be maintained, any hazards to be identified and made safe, working parties to be made conscious of hazards and to be appropriately skilled and aware, and that the work area is to be returned to normal conditions on completion of the work.
   b. No Packing materials are to be stored in the data centre. All unpacking of computer equipment is to be performed prior to entering the data centre. The recycling station that adjoins the bike shed to the NW of the data centre should be used to dispose of all rubbish and unwanted packing materials.
   c. A trolley is available for moving equipment into the data centre.
   d. Vacuum floor when necessary using power outlets labelled “No Computer Equipment”.
   e. Return all borrowed tools when work is finished or at the end of the day (whichever is sooner).
   f. 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 over night.
   g. No loose items, packaging, parts etc are to be stored in racks.
   h. Rack doors are to be secured following work or during times when rack is unattended. Racks are to remain unlocked.
i. Spare cage nuts, bolts, Velcro ties, etc are to be placed in the appropriate boxes on the shelves inside the data centre. Any damaged nuts/bolts should be disposed of.

j. Protect your feet. Ensure your footwear is appropriate for the activity you are undertaking in the data centre.

k. Protect your ears. The data centre is a noisy environment and includes high noise spots for which hearing protection is a requirement for extended exposure to the noise. Disposable earplugs are available for users on the shelves immediately inside the data centre.

l. Protect your eyes. The lasers associated with optical fibre communication systems in the data centre present an eye safety risk. Adhere to all warnings on devices and exercise caution when working with lasers.

3. Visitors must be accompanied by an authorised staff member.

4. There is a Telephone in the data centre that is available for users as required.

5. Data Centre Tours
   a. Tours should be notified at least 24 hours in advance. More notice is preferable.
   b. Tours will only be allowed with accompanying staff. Those staff 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 current work areas or safety hazards will be identified and access restricted.

6. New staff/contractor induction
   Before leaving any new staff member, contractor, or outside visitor in the data centre the following things must be explained to them.
   a. Explain how the lighting works.
   b. Point out fire exits.
   c. Point out building security, especially automatic door locking times.
   d. Point out non-essential power points labeled “No Computer Equipment” (for power tools, vacuum cleaner, laptops etc.).

2.3 Equipment Installation and Removal
The following section details the responsibility of data centre users regarding the installation and removal of equipment in racks. All tools and parts required for equipment installation, including cage nuts/bolts, fibre fly leads, UTP fly leads, power leads etc, are located on the shelves and table in the data centre. Users are free to help themselves to these for use in the data centre as needed.

2.3.1 Notification
Users must discuss with FMS any new work they wish to perform in the data centre. This enables FMS to organise the purchasing and preparatory work necessary to facilitate new works. Users should provide FMS with the following details.
1. Extent of footprint of work.
2. Timetable for work.
3. Expected heat density in racks initially and over the rack’s life cycle.
4. Power requirements of equipment initially and over the rack’s life cycle.
5. UTP and fibre requirements of equipment.
7. Any special requirements for installed equipment.

2.3.2 Layout of Equipment
FMS are responsible for overall room layout and configuration. Data centre users are responsible for the installation of their equipment in racks. The following points must be adhered to during the installation of equipment.

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 behind preinstalled UTP patch strips, FOBOTs, horizontal cable tidies or management switches.

2.3.3 Power
The Crisp Data Centre utilises an APC hot aisle containment system to provide integrated power and cooling to the computer equipment installed in the data centre. The system has UPS backup power 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.

Each rack within the data centre utilises two power distribution units (PDUs), each powered by one of two UPSs. Each PDU provides twenty 10 amp power outlets and four 15 amp power outlets. All PDUs are monitored via FMS software. Power thresholds are in place and FMS receive notification when 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 FMS.
2. The shortest power lead practical is to be used for the job.
3. Power leads are to be routed through vertical cable tidies as appropriate.
4. The total load on a PDU must not exceed 16 amps (displayed on PDU).
5. The total load on any bank on a PDU must not exceed 8 amps (displayed on PDU).
6. No extension leads or power boards are to be used in racks.
7. PDU’s are not to be moved between racks except by FMS.
8. Users will not have access to the switching function on PDUs.
9. Power leads for redundantly powered devices should be split one into each of the two PDUs in the rack.
10. Power leads must not cross between banks on PDUs. That is, power leads from the same device will be into bank 1 on both PDUs, or bank 2 on both PDUs within a rack.
2.3.4 Cooling

FMS are responsible for the design and implementation of the air conditioning strategy within the data centre. The hot aisle containment system uses chilled water in-row cooling units to draw hot air from the rear of racks in the hot aisle and eject ambient air at the front of racks into the data centre. The effective operation of the hot aisle containment system is dependent on the following criteria being met.

1. The front panel of in-row cooling units are to be used only by FMS.
2. Rack doors must be closed on completion of work.
3. The door into the hot aisle is not to be left open.
4. Horizontal blanking panels must not be removed from the front of racks except to allow the installation of computer equipment.

2.3.5 UTP and Fibre Patching

FMS will fit out racks with UTP patch strips and FOBOTs sufficient to meet the expected demand for each rack. Users will be responsible for the following:

1. The shortest patch lead practical is to be used for the job.
2. Patch leads must be routed through horizontal and vertical cable tidies as appropriate.
3. UTP and fibre have separate horizontal cable tidies.
4. No patch leads are to be run between racks.
5. No patch leads other than those supplied on the shelves in the data centre are to be used in the data centre.
6. Patches are to be split evenly to the left and right into vertical cable tidies. For example, on a 24 port UTP patch strip cables should be routed as follows;
   - Ports 1-6 and 13-18 should be routed to the left.
   - Ports 7-12 and 19-24 should be routed to the right.

2.3.6 Faults

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

1. If a user believes there is a fault with a piece of data centre infrastructure, they should report it to FMS. Users should not attempt to rectify such faults themselves.
2. Any faults arising from work in the data centre should be reported to the affected party and to FMS.

2.3.7 Completion of Works

Following the completion of work performed in the data centre, users must notify FMS who will inspect the work for compliance with these standards.
3 Facilities Audit and Change Management
The FMS will undertake a facilities audit of the data centre from time to time, and at least once per year, to review heat and power loads and their distribution within the room. Audit outcomes may include a need to upgrade, replace or rearrange facilities to maintain the whole-of-room environment. Changes requirements will be discussed with all data centre stakeholders and plans developed to effect the required changes with minimum service impact.

4 Security
Many users have a presence in the Data Centre and security is of utmost importance. CARDAX readers are installed on entrance doors controlling access and enabling auditing. Users should ensure that doors are closed securely when entering and leaving the data centre. Security cameras are also installed in the Crisp Data Centre monitoring both access to the data centre and to racks.

If users have any questions regarding what is expected from them, or are unable to comply with any point detailed in this document, they should consult FMS.