University of South Australia

Data Centre Access and Management Policy

Responsible Officer:	Deputy Director: Infrastructure & Cyber Security
Last Updated:	September 2021
Date of Review:	September 2024
Audience/Application:	IT and Facilities Management Staff
Related Documents	Acceptable Use of Information Technology (C-22)

1. PURPOSE

This policy governs physical access to the University's Data Centres.

Throughout this policy the term "Data Centre" refers to one of the controlled locations indicated below:

Campus	Data Centre	Physical Access Control	Fire Suppression
Mawson Lakes	E1-16	CARDAX	**Yes**
City East	C3-25B	CARDAX	No
Magill	A1-23	CARDAX	No
City West	DP1-27	CARDAX	**Yes**
City West	EM1-05	CARDAX	No
Whyalla	MB2-58A	Key	No

Note: Mawson Lakes and City West Data Centres are equipped with a VESDA (Very Early Smoke Detection Apparatus) with a fire suppressant FM200 gas release system. Successful completion of Fire and Security induction training is a pre-requisite for entry into the Mawson Lakes and City West Data Centres.

2. ONGOING ACCESS

Ongoing access will only be granted to IT staff and Security Officers who have a demonstrated need to access the Data Centre. The determination of who is granted access will be made on a case by case basis. If a staff member is not granted access to a Data Centre and still believes they require access, they may apply to the Chief Information Officer (CIO) in writing who will make the final decision on whether the requested access will be granted.

Ongoing access will be reviewed on a regular basis by the Deputy Director: Infrastructure & Cyber Security.

Only the individuals nominated in **Appendix A: Responsible Persons** may authorise ongoing access to a Data Centre. Responsible Persons must have completed any required induction, VESDA, and/or security training for the Data Centre they are authorising ongoing access.

Security Officers do not have authority to grant access to Data Centres to staff or any other third party, either on a temporary or permanent basis, with exception under Emergency Access conditions.

University of South Australia

3. ESCORTED ACCESS (BUSINESS HOURS)

Staff who have ongoing access to the Data Centre in accordance may escort a third party (e.g. a staff member without ongoing access, external contractor etc.) into the Data Centre during business hours provided that:

- Approval is granted by a Responsible Person (as defined in **Appendix A: Responsible Persons**) at least one working day prior to the day access is required. A Responsible Person may authorise access at shorter notice at their discretion but approval must be sought prior to the day access is required (see exceptions for Emergency Access).
- Third parties sign the visitor's book near the Data Centre entrance on arrival. In the case of a group visit the inducted person can sign on their behalf.
- The third party must be familiar with the 'acceptable behaviour' requirements of this policy.
- Staff with ongoing access are responsible for the activities of third parties during their visit, and
- Third parties sign out at the end of their temporary access. In the case of a group visit, the inducted person can sign on their behalf.

In the case of Data Centres equipped with a VESDA gas release system (Mawson Lakes and City West) the staff member with ongoing access must make sure that third parties are familiar with the Standard Operating Procedure (SOP) for the VESDA system before they are allowed to enter.

It is expected that staff members who request approval for a third party to access the computer room will remain with the third party while the third party is in the data centre.

4. AFTER HOURS ACCESS

Business hours are defined as 8am-6pm, Monday to Friday(excluding public holidays). 'After-hours' is defined as outside of this time.

Staff who have ongoing access to the Data Centre during business hours will also have after-hours access. If these staff require access to a Data Centre after-hours they are required to:

- Log the time in and out in the visitors log book;
- Only admit themselves and not third parties;
- Ensure their Manager (for ISTS staff) or a Responsible Person (for non-ISTS staff) is aware that they are accessing the Data Centre (either through overtime approval or if unplanned, by getting approval from a Responsible Person); and
- Notify on-campus security if they are the sole person accessing the Data Centre. (OHS&W requirement).

5. CONTRACTOR ACCESS

Extended access is sometimes required to the Data Centre for the purposes of major construction, installation and maintenance of services (air-conditioning, power, structural, etc.) or other approved activities.

Extended access to the Data Centre to undertake this work may be provided to Contractors if:

- The request is made to a Responsible Person at least 2 working days prior to the day access is required;
- A Responsible Person, or nominee, provides a WHS induction to contractors (Working Safely at UniSA) who have not undergone UniSA's induction process, and
- The request is approved by a Responsible Person;
- In the case of Data Centres equipped with a VESDA gas release system (Mawson Lakes and City West):
    - All contractors must have completed the ISTS VESDA fire and security induction/training.
    - All contractors have read and understand the contractor and ISTS SOPs.
    - Security Staff are satisfied that all conditions have been met and may determine, using their own SOP, that isolation of the VESDA is necessary.

The Responsible Person, or nominee, will be responsible for the activities and management of contractors for the period that the contractors are provided with access.

At the discretion of the Responsible Person, a temporary Cardax card may be provided for the contractor. Security will administer the release and return of these cards upon receipt of a formal request from a Responsible Person. If arrangements have not been made in advance the Security person on duty should contact a Responsible Person via phone to obtain approval. Short notice access is not guaranteed and all conditions of access still apply.

6. EMERGENCY ACCESS

Security Officers can permit emergency access for Fire, Ambulance or Police upon confirming identification and the existence of a genuine emergency.

Emergency access for other non-approved staff must be approved by a Responsible Person. If this emergency access is after hours it may incur overtime costs if it is deemed that an ISTS staff member needs to attend.

7. ACCEPTABLE BEHAVIOUR

Staff who have ongoing access to a Data Centre must:

- not delegate their approval to anyone else.
- immediately report any fault conditions they find or cause within the room to the IT Help Desk.
- immediately report any security related observations to a Responsible Person (see Appendix A).
- minimise entry and exit to the Data Centre by remotely administering equipment wherever possible and by considering temporarily removing equipment from the Data Centre if extended physical access is required.
- not provide any access (escorted or otherwise) to anyone else without prior approval from a Responsible Person (see **Appendix A: Responsible Persons**).
- not keep any door (into or within the Data Centre) propped open (using a physical device) unless pre-arranged with a Responsible Person.
- ensure that the Data Centre is secure at all times.

- not interfere with, disconnect or attempt to subvert any security or monitoring device within the Data Centre.
- not engage in any image or voice recording while in the Data Centre unless approved in advance by the Chief Information Officer or their delegate.
- observe safe work practices in accordance with WHS guidelines at all times.
- not unpack equipment in the Data Centre.
- remove any waste material that results from their activities as soon as the work is completed.
- ensure that the Data Centre is not used as a store and that only operational equipment is left in the Data Centre.
- not connect to any other network (apart from the University network) without approval by a Responsible Person.
- not interfere with any other equipment apart from that which they have a legitimate reason to work on.
- not remove or install equipment in the room without prior approval from a Responsible Person.
- not remove floor tiles unless the approved work requires this and it has been pre-arranged with a Responsible Person or for ISTS staff, undergone appropriate change procedures.
- not smoke, eat or drink in the Data Centre.
- gain approval from a Responsible Person for activities that may generate smoke, heat, dust and will require isolation of the VESDA sensors by Security.
- gain approval from a Responsible Person in advance for activities involving liquid, Electromagnetic Fields EMF (with the exception of mobile phone usage) or any other potentially hazardous consequences so that appropriate steps can be taken to minimise risk to sensitive equipment.

8. MONITORING

Data Centres contain video cameras.

Video cameras may be monitored in real time by ISTS staff and University Security Officers.

While video cameras are not constantly monitored by ISTS or University Security Officers, all activity in the room will be recorded. Video camera recordings will be retained for 30 days.

Written permission from the Chief Information Officer (CIO) or delegate is required for access to recorded material, outside of ISTS nominated staff or University Security Officers

Logs will be used to record access to monitoring systems and stored video. Logs are checked monthly for access to recorded data and monitoring.

9. COMPLIANCE

Failure to comply with this policy may lead to ongoing denial of access to the University's Data Centres and further disciplinary action where applicable.

University of South Australia

10. Appendix A: Responsible Persons

Person	Campus	Ext	Mobile
Karl Sellmann Deputy Director: ICT Infrastructure & Cyber Security	All	26363	0401 683 648
Tracy Deane Deputy Director: ICT Support Services	All	25221	0417 887 519
Carlene Reid Manager: Network Services	All	23060	0407 503 050
Brett Heritage Acting Manager: Systems Infrastructure	All	25098	0404 429 583
Jason Davis Coordinator – Network Services	All	23716	0417 868 409
Tristan Bibbo Manager: Cyber Security	All	22287	0401 673 302
Michael Staats IT Campus Manager: (Suburban & Regional)	All	22233	0406 453 077
Ricky Critcher IT Campus Manager: (City Campuses)	All	22177	0419 816 718
The Chief Information Officer (CIO) has overarching responsibility for all ISTS functions and is therefore a Responsible Person. **However, the Chief Information Officer (CIO) should only be contacted when those on the list above have been exhausted.**			
Paul Sherlock Chief Information Officer (CIO)	All	23575	0407 726 762