Data Centre Access Policy

Policy Name – Data Centre Access Policy	
Version number: 4.0	
Policy Owner	**Policy Author/Reviewer**
Digital Governance Risk & Compliance	Steve Coyle Digital GRC
Approving body	**Date of approval**
Digital Services Directorate	28/04/2023
	Equality Screened
	Yes
	Next Review date
	January 2026
Queries relating to this document should be directed to the Policy Owner – Digital Governance, Risk & Compliance via the Digital Services IT Service Desk https://www.ulster.ac.uk/ds/getting-help/service-desk. This document can be made available on request, in alternative formats and in minority languages to meet the needs of those who are not fluent in English.	

Contents

1 AIMS, PURPOSE AND SCOPE 2
2 DEFINITIONS 3
3 POLICY STATEMENT 3
4 COMMUNICATION, IMPLEMENTATION AND TRAINING 4
4.1 Work-related (**Permanent**) 4
4.2 Contractor/Consultant/Visitor (**Temporary**) 4
4.3 Emergency (**Temporary**) 5
5 COMPLAINTS PROCEDURE 5
6 RELEVANT LEGISLATION 5
7 RELATED POLICY DOCUMENTS REFERENCED 6
8 CONTACT DETAILS 6
9 APPENDIX A: DS HEALTH AND SAFETY POLICY GUIDELINES 7
10 APPENDIX B: GUIDELINES FOR STAFF ENTERING DATA CENTRE ROOMS 8
11 DOCUMENT HISTORY 9

1 AIMS, PURPOSE & SCOPE

This policy sets out the controls and rules that govern access to DS Data Centre room environments within Ulster University. These are required as there are times when people require access to carry out their duties or are paid to carry out changes to the environment or the hosted equipment within these secure areas.

Aims:

- To enable staff entering the room to perform authorised duties
- To enable contractors to enter the room and perform authorised duties
- To establish rules for conduct that must be observed by all people entering a Data Centre room (Appendix B)
- To keep appropriate records of Data Centre room activities
- To provide health and safety guidelines for staff entering Data Centre rooms (Appendix A)

It establishes the following rules:

- Requirements of people entering Data Centre rooms.
- DS staff responsibility.
- Record keeping requirements.

Purpose:
The policy is required because of the need to provide both access and high levels of security to these locations as they host “core business” computer and network systems and associated software.

Scope:
This policy applies to Data Centre rooms falling under the responsibility of Information Services and it has the approval of the Deputy Director of Finance & Information Services (DS).

It establishes the process to authorise the following to access Data Centre rooms in the following situations:

- Work-related access that cannot be undertaken by other means, for example via a networked and secure desktop computer. Typically covers physical access to hardware and work to the physical environment.
- Faculty/Department staff access
- Contractor/Consultant access.
- Visitor access
- Emergency access.

DS Campus Data Centres

- Belfast
    - Card-based access system controlled by Estate Services – authorization is given by ICT Infrastructure staff and affected by Campus Facilities & Services Manager (Belfast)
- Jordanstown
- Coleraine
- Magee

All Data Centres are controlled by the main University door access control system.

Note: Security have access to the Data Centres for out-of-hours emergency contractor access.

2 DEFINITIONS

DS – Digital Services
ICT Infrastructure – Division within DS responsible for the University's Data Centres

3 POLICY STATEMENT

There shall be no unauthorised access to any University Data Centre without an arranged request to the Data Centre & Operations Manager and under the supervision of an Infrastructure team member.

Violations of the conditions listed below may result in disciplinary action under the University's disciplinary procedures for a member of university staff or withdrawal of any future access for any contracted persons.

4 COMMUNICATION, IMPLEMENTATION & TRAINING

4.1 Work-related (**Permanent**)

Permanent card-based access to Data Centre rooms must only be authorised by the Enterprise Infrastructure Manager or Network Manager.

A request should be made via the Digital Services IT Service Desk with the following detail:

a) The person's name
b) The department or section where they are located
c) To which Data Centre they require access
d) The reason they require this access
e) From when access is required
f) For what period is access required
g) Frequency of access

Subject to approval users will be granted access to their requested Data Centre.
An access register shall be maintained by the Infrastructure Team. This register is reviewed on a regular basis by the Infrastructure Team.

All users must read and agree to the conditions set on in Appendix B. A copy is located beside the Visitor Logbook at each Data Centre door.

Access to secure areas will be monitored by Estate Services and can include (but not limited to)

- Audited door access control
- CCTV
- Intruder/Security Systems

4.2 Contractor/Consultant/Visitor (**Temporary**)

Contractors, consultants, or visitors that may require access to a Data Hall frequently or infrequently but do not satisfy the conditions of gaining permanent access, for example any third party.

For them to obtain access, the following best practice must be satisfied:

- They must have a business reason to require physical access to the Data Hall that satisfies the Enterprise Infrastructure/Network Manager.
- They must sufficiently notice to allow access to be considered and supervision to be arranged. This must be requested to the Enterprise Infrastructure Manager/Network Manager.
- Access will only be considered during university core hours, which are considered as weekdays between 8.45am and 5pm.

- Users granted temporary access will be supervised at all times by someone who has permanent access to the Data Hall. The supervising member of staff assumes responsibility for the visitor's actions.

The person supervising the visitor will be responsible for the following:

1. Visitor to adhere to Appendix B
2. Ensuring the visitor signs in and out of the Data Centre using the logbook located at the Data Centre door.
3. To observe and monitor the activities of this person in the Data Centre room at all times.

Note that for minor works requested by DS but executed by Estate Services, either using their own or contracted staff, all such works must have an accompanying suite of Methods Statements as a mandatory constituent of any associated project documentation. The responsibility to provide will reside with Estate Services and the responsibility to ensure its provision resides with the authorised Infrastructure Manager who is responsible for requesting the works.

4.3 Emergency (**Temporary**)

- In the event of an emergency out of core hours security should contact Estates Services Department
- If the emergency does not involve/affect any Digital Services related infrastructure or services, the attending Estates officer must report the details to the Digital Services next working day.
- If the emergency does involve/affect any Digital Services related infrastructure or services the Estates Officer should use on-call process,
- The Estates Officer is responsible for the emergency temporary access of contractors/visitors and must ensure that the temporary access responsibilities above are adhered to.

5 COMPLAINTS PROCEEDURE

If there are objections to this policy, these must be given in writing to the Deputy Chief Digital and Information Officer (Digital Services).

6 RELEVANT LEGISLAITON

See Applicable Legislation Ulster University

7 RELATED POLICY DOCUMENTS

Documents which must be read prior to first entering any of the Data Centres is:

- Evacuation Procedures Relating to University Data Centres
- Physical Security Standard

Other Internal Relative Documents for University Staff:

- DS Hardware Commissioning and Installation Business Process
- H&S Risk assessments for the following can be obtained from the Data Centre & Operations Manager
- Risk Assessment on Data Centres
- Risk Assessment on Installation of Network Switches into Data Centre Racks
- Risk Assessment on Installation of servers into Data Centre Racks

Additional information on Health, Safety and Wellbeing can be found on Digital Services HSW SharePoint.

8 CONTACT DETAILS

ICT Governance via the Digital Services IT Service Desk
https://www.ulster.ac.uk/ds/getting-help/service-desk

Security: In case of Emergency telephone 028 70123456

9 APPENDIX A

DS HEALTH AND SAFETY POLICY GUIDELINES

Key objectives include preventing accidents and injuries, minimise loss and to provide a safe place to work, when necessary. Members of staff with access to Data Centre rooms should always be very aware of any risks to themselves and others.

Our objectives are to: -

- Set down standards which will protect the health and safety of anyone entering Data Centre rooms.
- Have a working environment that is, as far as is possible, without risk to health and safety.
- Ensure that any guidelines in place are adhered to at all times.
- Carry out regular health and safety, fire checks, risk assessments and Portable Appliance Tests (PAT)

10 APPENDIX B

GUIDELINES FOR STAFF ENTERING DATA CENTRE ROOMS

Staff must always:

- Only permit access to authorised people
- Observe all safety rules, procedures, and instructions.
- Have separate area for storing and unpackaging equipment.
- Use all work items and equipment appropriately.
- Ensure 'good housekeeping' routines.
- Keep area clear of obstructions and packaging.
- Report any observed defects/damage to equipment.
- Report any hazards that come to their attention.
- Vacate premises immediately if alarms sound.
- Report stolen, lost or damaged cards to Data Centre & Operations Manager.
- Immediately report any accidents or serious incidents.

Staff must not:

- Install or leave cables or other items within the area of designated walkways or access points that may constitute a tripping hazard.
- Saw, grind, or cut materials in or around the vicinity of Data Centre rooms.
- Lend their access card or keys to anyone.
- Misuse/abuse equipment.
- Attempt to lift heavy objects alone.
- Use Data Centre room as storage area.
- Re-enter Data Centre room after any incident, until given all clear.
- Eat or drink while in the room.
- Allow unauthorised persons access to Data Centre room.

Things to do prior to, and upon, entering Data Centre room:

- Familiarise self with evacuation procedures on outer door.
- Locate nearest First Aid box before entering Data Centre room.
- Find out where recognised First Aiders can be located.
- Check Fire Extinguisher locations.
- Ensure that lighting and visibility is good.
- Check that noise levels are not inordinately high.
- Check that any possible escape routes are not blocked.
- Check floor for tiles not being in place.
- Check that carpet on tiles does not pose possible danger, i.e., tripping.
    - If working alone ensure that at least one other person, preferably your Line Manager knows where you are.

11 DOCUMENT HISTORY

Author	Status	Version	Date	Description
ICT Governance (SC)	Published	4.0	03/10/2024	Re-templated & Forwarded to OUS for Publication