# ITS Data Centre Access Procedure

**Access to the ITS Data Centres (DC) is arranged by Steve Silver, Infrastructure & Data Centre Service Owner (I&DC SO) in IT Services, Campus Security and ancillary services.**

# IT Services personnel

* Access requests must be authorised by the applicants Line Manager and a valid reason for access must be given. Such as, they have server equipment within the DC.
* Physical permission is not granted if the access protocol steps above are not followed.
* A valid university ID card is required to gain access to the DC. The University card alone will not provide physical access and the booking in visit procedure must be followed (see below)
* Due to the provision of Electronic door access on all cabinets within Argent Court Data centre, only specific individuals authorised to administer that equipment have access to the cabinets.
* If an individual leaves the University, their access rights across campus including access to data centres are revoked automatically upon their leaving date.
* They can also be revoked at any time by the individual’s line manager by making a request to the I&DC SO.

# Third Party maintenance tasks

Where access is required by a third party for maintenance as an example,

* Access requests must give at least 48 hours prior notice.
* The third party individual is escorted in to the DC by a member of the Infrastructure Team and they are not left unaccompanied at any time.
* Proof of the maintenance works must be provided. (RAMS)

# Management of access

All requests for permanent access are dealt with by the individual’s line manager and the I&DC SO, this cannot be circumvented. A deputy is appointed to fulfil access requests in the SOs absence.

# Booking the visit

An individual visiting the DC has to create a booking request to go into the DC.

Any request for 3rd party access, must be made at least 48 hours in advance.

* To book the visit an outlook calendar invite is sent by the person requiring the access; Each DC has a resource email account and is bookable in the same way a meeting room is.
* This must detail the individual’s name, the reason for the visit and the length of time required within the DC
* Doors to the data centre are strictly controlled by card access. There are no exceptions.
* Before entering the DC, the individual must contact Campus security to disable the intruder alarms. There is a phone outside each DC which is used to call campus security.

Campus Security keep auditable records of names and unique University ID number for security purposes. A transit report is available upon request from campus security, with a valid justification.

# Reporting, Signing in and out Records

* Upon entry into each DC, there is a signing in book which must be completed by each individual entering the DC. This document is available for viewing.
* CCTV covers all areas of the DCs, Footage is retained for 30 days and unless a valid request has been made for footage to be made available past the 30 days, the images are automatically erased.
* To view CCTV footage, requests must be made directly through Campus security.