ITS Datacentre Policy and services

Applicable to all ITS managed datacentres including

Argent Court Datacentre

University House Datacentre

ITS Chemistry (G block)

Author: Andy Hanif
Date: 24 February 2020

Version 2.

ITS Data Centre Policy

This document is intended as guidance for all persons who have access to any of the 3 ITS managed datacentres.

These include datacentres located in:

Argent Court
University House
ITS Chemistry (G block)

IT Services personnel (unsupervised access)

- Requests for unsupervised access must be authorised by the applicants Line Manager and a valid reason for access must be given. i.e. They have server equipment within the DC.
- 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 procedure must be followed (see below)
- Due to the provision of Electronic door access on all cabinets within all Data centres, 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 Infrastructure & Datacentre Service owner.

Booking datacentre visits

An individual visiting a Datacentre must create a booking request

- 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.

Signing in and out.

- Upon entry into each DC, there is a signing in book which must be completed by each individual. This document is available for review.

Lone worker policy

- Individuals are permitted to alone in the datacentres but they must adhere to the lone worker policy. The policy document is attached here.

Microsoft
PowerPoint Presenta

Third Party access

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

- Requests must give at least 48 hours prior notice – exceptions can be made for emergencies and these will be considered on a case by case basis.

- ALL third party individuals must escorted within the DC by a member of the Infrastructure Team (or their sponsor). They are not to be 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 Infrastructure & Datacentre Service Owner. This cannot be circumvented. A deputy is appointed to fulfil access requests in the SOs absence.

CCTV

- 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.

Deliveries

- Any deliveries must be advised with at least 48 hours' notice - exceptions can be made for emergencies and these will be considered on a case by case basis.

- Delivery vehicles must be equipped with tail lift where appropriate.

- A pallet truck can be provided by ITS services (at Argent Court datacentre)

Server lifters

- Mechanical and automatic server lifters are available for use in all datacentres. These must be used when installing and removing devices from racks. Training must be completed before use.

Ear defenders

- Ear defenders are available in all datacentres and can and should be used by all when appropriate.

Crash carts

- Crash carts consisting of monitor, keyboard, mouse and cables are available in all datacentres.

Unpacking of devices.

- All devices should be unpacked outside of the datacentre rooms. There should be no cardboard, paper or other combustible or dust causing materials left inside the machine rooms.

Rubbish removal

- All rubbish and packing materials associated with installation of devices must be removed and disposed of by the installer. Datacentre staff can assist with this, but it is not guaranteed and we may insist it is the responsibility of the installation person/team.

Fire alarm and suppression

- All datacentres are protected by fire detection and gas fire suppression systems. These are always set to Automatic. It is recommended that these are set to manual if individuals are working in the datacentre for any length of time. However, if the system is set to manual, it MUST be set back to Automatic/manual on exiting the datacentre. The systems are changed from Automatic/manual by way of the key located in the gas suppression control panel.

  If, for any reason the fire alarm is activated, then this will generate a loud audible alarm and flashing alarm lights. A warning that ‘gas release in 30 seconds’ will also be heard. At this point all individuals must leave the room within 30 seconds. It is possible to delay the release of fire suppression gas by pressing and holding the ‘gas hold off’ button next to the fire panel or by the exit door. If there is a genuine fire, the ‘gas hold off’ should only be used in an emergency i.e. to give people additional time to exit the room.