Article Number: 28 | Rating: Unrated | Last Updated: Wed, Aug 28, 2019 at 12:51 PM

Annex - VM and Colocation Terms

Colocation

Internet Central operates a number of special purpose areas around the country housing equipment providing critical IT Infrastructure to the organisation (referred in the rest of this document as 'data centres' or 'comms rooms'). As a part of IT Security, Data Protection and Service Availability best practice, this document defines the policies and procedures relating to access and conduct within Data Centre and Comms Room environments.

Access Procedure

To request access to a Data Centre, IC require an authorised customer contact to log into my.ic.uk and from services / colocation and fill in the form detailing the access. This is the case for planned and emergency access. This is to ensure that only customer authorised personnel have access to the DC.

Staff/Suppliers requiring assistance from the Internet Central for installation or removal of equipment will need to make sure this is requested at the same time the access request is raised.

Before leaving the premises, all visitors must sign out and return their access card to the card issuing reception and any packaging or waste must be removed from site. Packaging and waste is the responsibility of the 3rd party to lawfully dispose of, unless agreed in advance with Internet Central

Permitted Persons

A customer will nominate an administrative contact who controls the list of people with DC Access for the customer (this is the main admin contact for my.ic.uk).

The list of people with DC Access privileges is held on my.ic.uk
People on this list can request access to the DC for visitors (on the list or not.)

Staff against the main site will have access to all DC locations

DC locations can be linked to separate sites and specific staff members so that those staff are only allowed to request access for that location.

Access Restrictions

The following restrictions will apply to **all visitors**:

- Visitors without proper authorisation will be refused access
- Visitors who fail to present ID will be refused access
- All visitors requesting access must comply with the rules of conduct
- All visitors must comply with health and safety policies in place within the data centres
- Visitors deliberately attempting to access areas not permitted by their pass may be asked to leave and future access requests may not be approved.

The following restrictions apply to external **suppliers and contractors:**

- All suppliers must provide method statements and risk assessments in order to work. Suppliers not providing this documentation 24 hours prior to the requested time will be refused access (exceptions may be made in emergency situations but supervision will be required).
- Access to critical systems, such as power and cooling, will only be granted to approved maintenance contractors. Additionally, suppliers working in the plant rooms must have 2 people present at all times, or otherwise comply with any lone working arrangements agreed with the Estates team.
- Suppliers will be responsible for providing their own tools and personal protective equipment (PPE) for the work being undertaken, as well as any barriers or signage indicated in the agreed Risk Assessment and Method Statements.
- Suppliers will be asked to provide details of their public liability and indemnity insurances, refusal to provide these will result in access not being granted.

Rules of Conduct

Internet Central expects all employees, visitors and third parties to adhere to the organisations rules of conduct when working in Data Centre and Comms rooms.

The following rules are compulsory and may carry penalties or future restrictions if breached:

Physical Access / Health and Safety

- Unauthorised access is strictly prohibited;
- Food, drinks and smoking are strictly prohibited within the data centre;
- Cardboard and other forms of packaging must not be stored or otherwise left inside the Data Centre or Communications/Hub Rooms;
- All visitors may be requested to submit to a search of tool and laptop bags by security, prior to, or following access to the Data Centre or Comms rooms;
- When accessing the Primary Data Centre, staff/visitors must ensure they are trained and familiar with the correct operation of the Fire Suppression system, or are otherwise accompanied by a member of staff who is trained;
- When working inside cold/hot aisles or in cold/hot air plenums, staff and suppliers should ensure that disruption to the cooling process is minimised; Specifically, aisle doors should be closed as soon as it practical and not left open.
- Tools such as drills or soldering irons and/or planned work that may produce vibrations, debris, dust, moisture, smoke, high temperatures or static electricity are not permitted without prior written authorisation from Internet Central;
- When work has been completed, any racks worked in must be left closed and locked. Aisle doors must be closed. Any rubbish or debris should be removed, and the area left safe, clean and tidy. Fire Suppression should be re-armed (if applicable).
- Accidents and Near Misses **MUST BE REPORTED TO IC**

Good Citizen

- Do not alter or change the Core equipment:
    - Air conditioning.
    - Electrical distribution.
    - Fire suppression.
    - Environmental and other monitoring.
    - Routing and networking equipment.
- You are responsible for retaining copies of your own data. Internet Central will not automatically keep backups of your data unless expressly stated in the contract.
- Internet Central accepts no responsibility for loss of data, information in any form or other matters whatsoever which result from the use of this service.
- You are responsible for the content of your servers, including obtaining the legal permission for any works they include and ensuring that the contents of these pages do not violate English law.
- You are responsible ensuring that software and operating systems on your servers are correctly and properly licenced. (VMs supplied by IC have an OS licence as part of the contract)

- You will be held responsible for and accept responsibility for any defamatory, confidential, secret or other proprietary material available via your server.
- Any collection of personal data must be in accordance with the Data Protection Act and the Data Protection Principles.
- Especially in shared rack locations, suppliers must ensure they take care to not interfere with other equipment. If there are any concerns a member of Internet Central staff should be contacted who will assist;
- Use of any equipment that will adversely affect other equipment within or users of the DC is not permitted.
- You may not advertise your Web site / service, or cause another person to advertise it, by techniques that would be classified as abuse if they were carried out from an Internet Central Account. This includes, but is not limited to, bulk spam emailing and excessive social media posting. Such action may be treated under the appropriate AUP as if it had been done from the Account, or as a violation of this AUP or both.
- If your account is barred for any reason (e.g. non-payment) access to your service may be suspended.
- Internet Central reserve the right to vary the definition of 'over usage' at their sole discretion at any time without prior notice.
- Internet Central reserve the right to impose limits on or charge for over usage of Bandwidth at its sole discretion.
- Internet Central reserve the right to impose limits on or charge for over usage of Power at its sole discretion.
- By locating your servers with Internet Central (physical or virtual), you will be deemed to have agreed to and accepted the terms and conditions of use of the service.
- The IP address that may be allocated to your Web site may be changed or withdrawn at any time without notice. The IP addresses allocated to a service remain the property of Internet Central.
- Internet Central reserve the right to vary the Conditions of Use and acceptable use policy for the service at their sole discretion at any time and without prior notice.
- Any decision made by Internet Central in relation to this service shall be final.

Document revision 7.0 28/08/2019

Posted by: Mark Simcoe - Tue, Jul 25, 2017 at 3:32 PM. This article has been viewed 2134 times.

Online URL: https://kb.ic.uk/article/annex-vm-and-colocation-terms-28.html