



Node4 Data Centre Access Procedure ISO9001/27001

PUBLIC
NODE4 LIMITED
31/05/2016

DATA CENTRE ACCESS AND SECURITY

INTRODUCTION

Node4 take the security of our data centre environment and the information assets stored within it very seriously.

As such, only authorised personnel will be allowed into the data centre to access servers and other equipment. This document outlines the process for obtaining access to our data centre and rules for subsequent visits.

Please read this document carefully as these rules and guidelines are in place to protect your data and equipment.

Node4 operate in accordance with ISO9001/27001 policies and procedure and we adhere to the physical security recommendations of the PCI security standards (section 9).

REQUESTING ACCESS

As a Node4 customer, you can request access to your racks via our helpdesk 24/7/365. To raise an access request, you will need to be a registered user on our helpdesk and have the permission on your account to do so. The following details how to become a registered user and how to obtain access:

1. Initially one customer account administrator needs to be registered, this will be completed during your first order with us or by sending an email to your account manager providing the email, job title, DDI and mobile number of the user to be registered.
2. Once registered the administrator user can then raise additional user account requests by logging in to our helpdesk and raising a support ticket. When raising requests for new users you will need to specify their email, job title, DDI and mobile number and their user account levels:

User can request DC access for self (Y/N),

User can request DC access for others (Y/N),

User can request new user accounts (Y/N) (Administrator accounts)

(Please note that if authorised people leave your organisation it is up to you to inform Node4)

3. Visits to the data centre will require an access request from an authorised user on the helpdesk system, logs of which are stored for a minimum of six months. We ask that access requests are raised at least 24 hours prior to the visit.

Access requests must contain the following information:

- Company name
- Visitor(s) name
- Visitor mobile number
- Reason for visit
- Vehicle registration number
- Estimated arrival time
- Estimated time required on site
- Date of visit
- Equipment removal
- Equipment installation
- Rack number(s)
- Which data centre (including the data hall) access is required for
- Do you have your own pass?

Access requests can be raised directly on the helpdesk (<https://support.node4.co.uk/>) or by emailing access@node4.co.uk from a registered user email.

For emergency access (email sent outside normal business hours 365/24/7) email emergencyaccess@node4.co.uk

Your access request will be authorised / denied by Node4 and confirmation will be emailed to you and the ticket updated. If your access is denied, a reason and escalation route will be given.

You will not be allowed into the data centre without a valid access request, pass or photo ID.

NODE4 CUSTOMER ID PASS

Customer can request their own visitor pass if they are a regular visitor to site. This pass will give you access to the data centre building upon a valid access request and will be enabled only for the duration of the visit and deactivated when not in use. If you lose this pass, please inform Node4 as soon as possible.

MULTIPLE DAY ACCESS REQUESTS

Each separate visit to the data centre must be accompanied by a separate access request ticket. We do not allow multiple day or open ended access requests. Multiple people can be named on the access request, but this should reflect the actual visitor list as closely as possible (i.e. not a list stating 1 or 2 engineers from a list of 10). This is done to improve audit trails and protect against unauthorised people (such as recent leavers) gaining access to the data centre.

VISITOR LISTS

It is your responsibility to maintain the list of people authorised to visit the data centre stored with Node4. If you wish to change the list of authorised people in your organisation that have access to the data centre, this should be done via a ticket. We can issue you with a list of authorised people on request.

ACCESS TO RACKS

Node4 racks are kept locked at all times. We will accompany you to your rack and unlock it for the duration of your visit. Most racks will self-lock when the doors are closed, but please check that racks are locked when you leave site. You will only be granted access to the racks requested on your helpdesk ticket. Additional rack access will require an amended or new ticket.

CCTV AND OTHER MONITORING

The Node4 data centre is fully covered by CCTV cameras. Images are time-stamped, recorded and stored for 3 months. A copy of our CCTV policy is available on our website. All swipe card activity is time-stamped, logged and kept for a minimum of 6 months.

REMOVABLE MEDIA

Node4 provide a fire safe for storing removable media on site. You can use this safe to store your own media for a fee (subject to space being available).

Node4 can provide facilities for safely destroying electronic and paper media that you no longer require.

GENERAL DATA CENTRE VISITOR RULES

- Present your photo ID at reception upon arrival to obtain your visitor pass and always sign in on the visitor log
- Please read and follow our data centre rules (including fire safety information). These are printed on your visitor pass
- Familiarise yourself with the building layout including exit routes
- Your visitor pass must be worn and visible at all times
- If we issue you with a temporary access card, we will keep your photo ID (e.g. driving license) for the duration of your visit
- Do not lend your pass or access card to other people
- Do not prop open doors or let other people “tailgate” you into the data centre
- Customers are responsible for the removal of all packaging that comes with their equipment. (Skips can be provided for an additional cost)
- Do not take packaging materials into the data halls and do not store flammable materials, such as cardboard boxes or paper, in your racks
- Customers must not interfere in any way with other customer’s racks, cabling, power or equipment
- Food and drink are not allowed in the data centre
- No Smoking onsite, except in designated smoking areas
- Always sign out of the building upon leaving (even if you are planning on returning)
- If you are unsure about anything, please ask a member of staff for assistance