NODE4 DATA CENTRE AND OFFICE ACCESS POLICY

INTEGRATED MANAGEMENT SYSTEM

Policy and Procedure

Public

14/10/2020

Data Centre and OFFICE ACCESS Security

INTRODUCTION

Node4 take the security of our data centre and office environments seriously and the information assets stored within it. As such, only authorised personnel will be allowed into the data centre and office, providing the necessary ID.

This document outlines the process on how to gain access to the data centres and the rules when on site.

Please read this document carefully as the rules and guidelines are in place to help avoid any delays when attending site and to protect your data, equipment and the environment they are in.

We operate in accordance with ISO27001 and Node4's Quality Management System policies and procedures; we also adhere to the physical security recommendations of the PCI security standards (section 9).

REQUESTING DATA CENTRE ACCESS

As a Node4 customer, you can request access to your racks via our service desk 24/7/365. To raise an access request, you will need to be a registered user on our service desk 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 first user to be registered.

2. Once registered, the new customer administrator user can then raise additional user account requests by logging on to our service desk 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:

Account-level options:

Primary Contact – This enables a view within the self-service portal to see ALL tickets raised by the company.

Data Centre Access – This enables the users to view and submit the Data Centre Access Request item through the self-service portal.

Contact Authoriser – This allows a user to submit requests for any user changes. For example, new users/removal of users/given primary contact or DC access.

Please note that if registered people leave your organisation, it is up to you to inform Node4 through the service desk so the registered user can be deleted.

3. Visits to the data centre will require an access request from an authorised user on the service desk system. We ask that access requests are raised **at least** 24 hours prior to the visit. **If the visit is an emergency and you cannot provide over 24 hours' notice, please raise the access request and immediately follow up with a call to our support number on 0845 123 2229** with the access reference and we will process and inform security promptly.

4. Please note in order to ensure a smooth sign in visitors are requested to have their access reference to hand and allow sufficient time for checks and sign in to be completed (we advise that this could take up to 30 minutes unless an emergency).

Node4 Limited | Millennium Way | Pride Park | Derby | DE24 8HZ | 0845 123 2222 | www.node4.co.uk

Data Access requests must contain the following information:

- **Visitor Name(s)**
- **Visitor Company Name(s)**
- **Visitor Phone Number(s)**
- **Reason for Visit**
- **Vehicle Registration Number(s)**
- **Visit Start Date & Time**
- **Hours Required on Site**
- **Will Equipment Be Installed?**
- **Will Equipment Be Removed?**
- **Which Data Centre Location?**
- **Which Rack Number(s)?**
- **Do You Have Your Own Pass?**

You can supply additional information at the end of the form also if required.

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

Access to sites may change due to specific events, such as Business Continuity, and visitors will be advised of any changes accordingly when booking their Access Request.

Office Access requests for meetings with Node4 personnel will be raised internally by Node4. Visitor(s) access to any of Node4's offices will only be granted once an internal request has been raised and authorised and gone through the appropriate process and security checks. Once site visitor access has been authorised a ticket case reference number will be issued and forward by email to the visitor(s).

EMERGENCY ACCESS

We appreciate that at times, emergency access is required and customers are unable to provide 24 hours of notice. For emergency access, please follow the standard procedure detailed above, follow up with a phone call to our support number 0845 123 2229. You will then need to provide the access reference, and that emergency access is required, we will then process the access request checks immediately to enable access.

VALID customer ID

You will not be allowed into the data centre or offices without a valid access request, pass or photo ID. The only valid photo ID that will be accepted by Node4 is a passport or driving licence. Failure to provide valid photo ID will result in your access being denied.

The following sites will be responsible for checking visitor ID

Derby Head Office and Data Centre - Receptionist

Wakefield Data Centre - Security Personnel / Receptionist

Northampton Data Centre – Security Personnel / Receptionist

Nottingham Office – Node4 authorised persons (list of trained Node authorised persons are displayed on the notice board in the reception area).

Reading Office – Receptionist

Node4 customer ID pass

Customers can request their own visitor pass to the Data Centre 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. Please note, the Node4 ID pass is not accepted as a photo ID when attending site, you will still need to provide government-issued photo ID of either a driving licence or passport.

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.

Registered Users

It is your responsibility to maintain the contact list of people registered on our service desk and therefore authorised to visit the data centre. 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 the site. You will only be granted access to the racks requested on your access request. Additional rack access will require a new access request to be raised.

CCTV and other Monitoring

The Node4 data centre is fully covered by CCTV cameras. Images are time-stamped, recorded and stored for three 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 and Office Visitor Rules

- Present your photo ID at reception upon arrival to obtain your visitor pass and always sign-in on the visitor log.
- If we issue you with a temporary access card, we will keep your photo ID (Driving license or Passport) for the duration of your visit.
- Please read and follow our data centre rules (including fire safety information). These are printed on the inside cover of the book when you sign in.
- Your visitor pass must be worn and visible always and displayed on your lanyard. The colours of the lanyard distinguish the individual on-site, grey = employee / green = visitor / blue = contractor.
- 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.
- Familiarise yourself with the building layout, including exit routes.
- If you are unsure about anything, please ask a member of staff for assistance.
- No Smoking on site, except in designated smoking areas.
- 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
- No cabling can be run outside of the customer racks.
- Food and drink are not allowed in the data centre.
- Always sign out of the building upon leaving (even if you are planning on returning) your photo ID will then be returned to you.