1. Contents

2. Overview

This document describes the procedure that anyone visiting the data centres should follow when requiring access.

The following sections contain the requirements all visitors must comply with to maintain the company's high level of security and integrity, and to ensure smooth operation of the facilities.

3. Introduction

Timico operate data centre facilities around the UK. All locations have access control and 247 CCTV monitoring. All locations can be accessed by customers, suppliers, and employees to carry out work on their respective equipment. Access to data centre locations may require an escort by an authorised Timico employee and is at the discretion of Timico.

Note: Escorted access may incur additional charges.

4. Rules of conduct

Timico expects all employees, visitors, and thirds parties to adhere to the company's rules of conduct when working in our data centres. Additional restrictions may apply to follow local and national government guidelines, please check at the time of booking.

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

- Food, drinks, and smoking (including e-cigarettes and vaping) are strictly prohibited within the data centre.
- All visitors to our data centre and office locations are encouraged to practice elevated levels of personal hygiene while on site and before arrival.
- Cardboard, combustible material and other forms of packaging or waste must not be left inside data halls, suites, or racks. Failure to do so may incur charges.
- All visitors must submit to a search of tool and laptop bags if requested by a member of security or engineering staff
- Tools such as drills, soldering irons or brazing that produce debris or smoke are only permitted by a hot works permit or permit to work.
- In shared rack or suite locations escorted access will be required and a charge may apply. Customers/suppliers will need to ensure they take care not to interfere with other equipment.
- When working inside aisle containment Pods customers and suppliers should ensure that the Pod doors are closed to maintain the cooling process.
- All equipment should be mounted for correct airflow. Air flows from the enclosed cold aisle or cold vent to the hot aisle. Provisions can be made for side venting equipment.
- When work has been completed, the rack must be left closed and locked unless customer requirements allow/permit otherwise.
- Cabling work between racks, or the lifting of floor tiles, must not be conducted without prior approval from the Timico Engineering team.
- Anyone found tampering with or working on any equipment without authorisation will be immediately removed from the building, the offending party maybe subject to prosecution and will be held liable for any damages or any operating costs associated with their actions.
- No photos are to be taken – photos can be requested from Timico to ensure customer confidentiality.
- Blanking plates and brush bars must be used to fill any gaps. Blanking plates can be requested from DC Reception or the Engineering team.
- Equipment with multiple power supplies must be connected to multiple PDU's within a rack.

5. Access request procedure

Customers and suppliers requiring access to the Data Centre should contact Timico's Network Operations Centre by emailing the request to access@timico.co.uk whereby an engineer will process the request, assign escort resource if required, and provide access code to the requester if required.

Emergencies and amendments: For requests that are urgent (less that 24h notice) we please ask that you the follow the procedure below then call our 24x7 support number on **0333 220 0222**. For amendments: reply to your confirmation, then call our 24x7 support as above quoting your reference number.

The following information is required to process the request:

- Company name or account number.
- Contact name and number of the requester.
- Name(s) of the person(s) requiring access.
- Data Centre location including Rack/cage details where access is required.
- Date/s access is required for.
- Estimated time of arrival.
- Expected duration of visit.
- Summary of work to be undertaken including any delivery or collection details and Timico point of contact if applicable.

All 3rd parties requiring access must, upon arrival, provide the original and valid photographic identification before access will be granted. We will only accept the following forms of identification:

- European photographic driving license.
- Valid passport.
- National identity card.
- Military identification.

Any other forms of ID must be reviewed by the Data Centre manager before they will be accepted and must contain a photo of the visitor. **Credit/Debit Cards are not acceptable forms of ID.**

Once visitors have signed in and identification has been validated, an electronic pass and visitors' badge will be issued allowing access to the designated area of work. Both items must always be clearly visible on your person and be presented upon request.

Note: Newark Data Centre uses biometric access control in addition to the electronic pass. Therefore, a scan of a fingerprint will be taken upon arrival.

Customers requiring assistance from Timico's engineering team for installation or removal of equipment will need to make sure this is requested at the same time as access is requested. This service may incur charges and is subject to availability. We ask that you give a minimum of 24-72 hours' notice when requesting assistance.

Before leaving the premises, all visitors must sign out and return their electronic pass to reception and any packaging or waste must be removed and deposited in the bins provided. Failure to do so may incur a charge.

6. GDPR

Timico will retain access profile and biometric data for customers requiring regular access to data centre locations. In line with our privacy policies Timico may retain a copy of photographic identification on file and a photograph will be taken on arrival to be stored against the access profile. The permanent access list will still require visitors to request access via the same process described.

Access profiles will be reviewed regularly. Users may have their profile and biometric data removed upon request and will require to be re-added on next arrival.

Our data retention policies

By accessing the Data Centres you are agreeing to the relevant Timico Privacy Policy and General terms and conditions where applicable. These can be found on our website at: https://www.timico.com/terms-policies/

7. Access exceptions & restrictions

The following restrictions will apply to all visitors:

- Visitors without proper authorisation will be refused access
- 24-hour notice or more must be given in advance of all non-essential access requests.
- Visitors who fail to present photographic 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 electronic pass will be asked to leave and future access requests may not be approved

The following restrictions apply to contractors working in the Data Centres:

- All contractors must provide method statements and risk assessments to work. Contractors not providing this documentation at least 24 hours prior to the requested time will be refused access (exceptions may be made in emergency situations, but supervision will be required)
- In shared locations escorted access may be required and a charge may apply.
- Facilities contractors may be required to complete a **Permit to Work** form before starting work and may have to be supervised.
- 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 always present.
- Suppliers will be responsible for providing their own tools and personal protective equipment (PPE) for the work being undertaken.
- 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.

8. Deliveries and Collections

Timico will accept deliveries and collections of customer equipment as part of an access request. When arranging a delivery, customers/suppliers must provide the number of parcels expected, the consignment number if known, the expected delivery date and the handling courier. The delivery ID issued must then be clearly marked on all parcels. Failure to do so may result in the parcel being refused. 24 hours' notice is requested in advance of any deliveries. Equipment will be held for up to 10 working days and charges will be incurred per day in excess of this period.

Delivery addresses can be confirmed at the time of request with Timico.

Note: Newport Data Centre. Any deliveries to this site must be scheduled with minimum of 24 hours' notice. Drivers are asked to phone 0333 220 0222 and ask for Telford Security team 30 mins before arrival.

9. Appendix

Newark Data Centre

Timico Limited
Brunel Business Park
Jessop Close
Newark
Nottinghamshire
NG24 2AG

London Data Centres

Digital Realty London
Sovereign House
227 Marsh Wall
London
E14 9SD

Equinix LD8
Harbour Exchange
8/9 Harbour Exchange
London
E14 9GE

Telford Data Centre

Timico Managed Services
Hortonwood 37, Donnington,
Telford
TF1 7GT

Newport Data Centre

Timico Managed Services
Audley Avenue Industrial
Estate,
Audley Ave
Newport
Shropshire
TF10 7BX

Additional information

- Onsite parking for visitors is provided at the front of the Newark, Telford, and Newport buildings.
- Break out areas and amenities are provided in locations with customer access.
- Patch and power cables can be provided upon request but may carry additional costs.
- Disabled access is catered for at all locations.