Data Centre Access Procedure

redcentric

AGILE • AVAILABLE • ASSURED

Applies to:	All visitors requiring access to Redcentric Data Centres, listed within this document in Section 3.2.
Date of Approval:	21June 2023

Document Control

Title	Data Centre Access Procedure
Originator / Author	Gwen Cooper / Andrea McCormack
Reviewer	Data Centre and Facilities Director
Business Area	Operations – Physical Security
Review Cycle	Annual

Change/Review Record

Version	Date	List Changes made to document	Change Ref	Document Status
Draft	2 August 2011	New document	NA	Final Draft
1.0	12 August 2011	Formatting/Branding/Version Control ready for release	NA	Obsolete
1.1	6 February 2012	Updates to including Reading facility.	CM244521	Obsolete
1.2	21 Jan 2013	Updated to include NHS & Local Authority issued ID	CM247972	Obsolete
1.3	21 June 2013	Updated re: mobile phone usage.	CM253195	Obsolete
1.3	3 January 2014	Reviewed, no changes required other than rebranding.	CM259162	Obsolete
1.4	24 June 2015	Update to acceptable photographic ID to include DWP photo ID.	DCR1105	Obsolete
1.5	19 Apr 2019	Change of reviewer	DCR1569	Obsolete
1.6	06 June 2022	Clarified driving license ID, added section 5 ‘Security’	DCR1882	Obsolete
1.7	19 May 2023	Added new Redcentric sites	DCR2023	Obsolete
1.8	16 June 2023	Amended applicability	DCR2034	Obsolete
1.9	21 June 2023	Added new Redcentric sites and changed document owner and reviewer.	DCR2041	Live

Document Ownership

Redcentric's Data Centre and Facilities Director is the owner of this document and is therefore responsible for ensuring that this policy is reviewed in line with the review requirements of Redcentric's ISO27001 Information Security Management System and PCI DSS requirements.

Contents

1 Introduction

Security is one of the most important services offered by Redcentric to our customers. Redcentric operates a secure access policy at data centres for all personnel, computer systems, peripherals, and networks.

2 Scope

This procedure applies to all of the Redcentric data centres listed within this document.

3 Access Security Controls

Access to Redcentric Data Centres is controlled 24x7x365 days/year via a series of visual & electronic access pass systems and procedures (pass readers).

There are 4 levels of security in operation:

1) Pre-arranged access
2) Building Security (Landlord)
3) Acceptable Photographic ID
4) Access Passes

3.1 Pre-arranged Access

Before access can be granted to any of Redcentric's Data Centres, you must first raise an access request with Redcentric Support. This can be raised by calling 0345 120 7070, by sending an email to support@redcentricplc.com or via our customer portal www.redcentricplc.com. Please provide a minimum of 24 hours' notice.

All access requests must be submitted by an authorised contact and must include the following information:

- Full names of all visitors attending
- Date and time of the visit
- Redcentric site and areas therein that the visitor(s) require access to. Please note that private hosting suite customers will only be able to access their own suite.
- Any special requirements - for example, a requirement to access under floor cables. In these circumstances, a member of the Facilities team may have to be present to marshal the works and ensure that isolations to fire detectors are put in place.
- Details of any equipment planned to be removed from/brought into the facility during the visit, which will be recorded in the interaction raised as this is a requirement of our Security Policy.

If under floor access is required, for example, for cable work, this needs to be stated in the access ticket and a Risk Assessment and Method Statement must be provided – this will be checked prior to the visit and must be approved by the Facilities department in advance of the visit. Where cable trays are provided, these must be used.

Once the access request has been recorded, an interaction reference number will be provided, which must be quoted by visitors upon arrival.

3.2 Building Security

3.2.1 Harrogate

Building Landlords provide the first level of security via the provision of Security personnel, who monitor the perimeter and common access areas of the building, via CCTV and patrols.

Building Reception staff sign-in visitors, issuing a building visitor pass, then notify Redcentric of the arrival of the visitor; the building visitor passes must be returned upon leaving the building.

If the visitor does not possess a permanent Redcentric Data Centre access pass, a Redcentric member of staff will escort the visitor to the Redcentric access pass issuing area.

Redcentric staff will check that a valid access request has been made for the visit and they will request a Government issued form of identification to validate and confirm identification of the visitor.

All Redcentric issued passes must be returned to Redcentric before leaving the data centre.

3.2.2 Reading

The first level of security is via the mantrap into the Reception area, the perimeter and Reception areas being monitored via CCTV.

Reception staff sign-in visitors, issuing a visitor pass, then notify the Redcentric resource concerned of the arrival of the visitor.

If Data Centre access has been requested, Reception staff will first check that a valid access request has been made for the visit and they will request a Government issued form of identification to validate and confirm identification of the visitor.

3.2.3 Shoreditch (London)

The first level of security is a call via an external intercom, to the onsite security team. Once the security guard has confirmed identification, the security guard will permit access to the visitor into an isolated Reception area.

The security guard will conduct the visitor access checks, including asking for a Government issued form of identification.

On successful completion of the visitors access checks, the security guard will issue the visitor a pass. The visitors pass issued will only provide access to the areas required.

Where required and or appropriate, the security team will notify the appropriate Redcentric resource(s) of the visitors arrival.

The visitor must return the pass issued by Redcentric security team, back to the security team before they leave the data centre.

3.2.4 Hounslow (LTC)

The first level of security is a call via an external intercom, on the vehicle barrier or turnstile. The Redcentric onsite security team will seek confirmation of access details before permitting access through the respective barrier. Once successful details have been confirmed with the Redcentric security team, they will permit access onto site.

The next level of security is access into the isolated reception area. The Redcentric security team have to permit visitors access into the reception area.

On arrival into Reception, the Redcentric security team will complete the visitor access checks. The visitor must provide a Government issued form of identification to the Redcentric security guards. On successful completion of the visitor access checks, the security guard will issue the visitor a pass. The visitors pass issued will only provide access to the areas required.

Where required and or appropriate, the security team will notify the appropriate Redcentric resource(s) of the visitors arrival.

The visitor must return the pass issued by Redcentric security team, back to the security team before they leave the data centre.

3.2.5 Woking (TC3)

Building Landlords (Digital Realty) provide the first level of security via the provision of Security personnel, who monitor the perimeter and common access areas of the building, via CCTV and patrols

Building security staff sign-in visitors, they will also validate the identity of the visitor. The visitor must provide a Government issued form of identification to the building security team for them to be issued with a site pass. Once visitor sign-in checks and processes have been completed, the building security team will then provide directions to the Redcentric reception area.

The pass issued by the building security team will only provide access to the common areas to access Redcentric, it will NOT provide access to the Redcentric data centre hall(s) within Woking (TC3)

On arrival at the Redcentric reception area within Working (TC3) Redcentric staff will also go through the visitors signing in process.

Once validation checks have completed, Redcentric Data Centre Operations will issue the visitor with a second site pass. The second pass that the visitor receives will provide access to the respective Redcentric data centre hall(s) within Woking (TC3).

The visitor must return the pass issued by Redcentric back to Redcentric reception. Separately, the visitor must return the pass issued by the building security team to the building security team.

3.2.6 Elland (TC4)

The first level of security is a call via an external intercom, to the onsite security team. Once the security guard has confirmed identification, the security guard will permit access to the visitor into an isolated Reception area.

The security guard will conduct the visitor access checks, including asking for a Government issued form of identification.

On successful completion of the visitors access checks, the security guard will issue the visitor a pass. The visitors pass issued will only provide access to the areas required.

Where required and or appropriate, the security team will notify the appropriate Redcentric resource(s) of the visitors arrival.

The visitor must return the pass issued by Redcentric security team, back to the security team before they leave the data centre.

3.2.7 Byfleet

During office hours the shared access gate that is set back from the main road is open and provides access into the data centre car park area.

Outside of office hours the shared access gate is closed and locked and is managed entirely by Redcentric. There is an Intercom on the perimeter gate, which goes through to the onsite Redcentric security guard. The security guard then manages ingress and egress access through the perimeter gate.

On arrival at the secure data centre reception, the Redcentric security guard will conduct the visitor access checks, including asking for a Government issued form of identification.

On successful completion of the visitors access checks, the security guard will issue the visitor a pass. The visitors pass issued will only provide access to the areas required.

Where required and or appropriate, the security team will notify the appropriate Redcentric resource(s) of the visitors arrival.

The visitor must return the pass issued by Redcentric security team, back to the security team before they leave the data centre.

3.2.8 Gatwick

External perimeter fencing provides the first level of security at the Redcentric Gatwick data centre, all visitors (arriving on foot or in a vehicle) are required to call the data centre reception via the external intercom installed on the perimeter fence.

Visitors will be requested to provide initial access details. Once initial details have been verified access will be provided to enter the data centre grounds/car park.

On arrival at the data centre reception, Redcentric staff must release the external door to provide access into a secure and segregated reception area. Further checks, including identification checks will be conducted including requesting a Government issued form of identification.

On successful completion of the visitors access checks, Redcentric will issue the visitor a pass. The visitors pass issued will only provide access to the areas required.

Where required and or appropriate, the security team will notify the appropriate Redcentric resource(s) of the visitors arrival.

The visitor must return the pass issued by Redcentric security team, back to the security team before they leave the data centre.

3.3 Government Issued Photographic ID

Examples of acceptable ID are:

- Valid UK Driving Licence (full or provisional)
- Valid UK Passport
- Government issued Contractor's Card
- Government issued (photographic) National Health Card
- DWP Government issued (photographic) ID
- National Health Card
- Valid Non-UK Driving Licence
- Valid Non-UK Passport

3.4 Alternative Acceptable Photographic ID

In addition to the Government Issued Photographic ID, the following are also acceptable:

- NHS issued employee photographic ID
- Local Authority issued employee photographic ID

UNDER NO CIRCUMSTANCES WILL ANY VISITOR BE ALLOWED INTO THE DATA CENTRE WITHOUT ACCEPTABLE PHOTOGRAPHIC ID AS THIS WOULD CONSTITUTE A BREACH OF OUR SECURITY POLICY.

3.5 Access Passes

The visitor will then be issued with a temporary access card for the specific area(s) stated in the access request; this will be recorded in the pass issuing log.

Access to Redcentric switch rooms and plant rooms can be requested for specific contractor visitors if required. In these circumstances the Facilities department must approve the request.

The Data Centre is zoned and controlled through a privileged level of access. When the visitor has left the building having returned the access pass, all of the access privileges assigned to the pass are immediately disabled and the pass stored in a secure cabinet.

Access pass movements are recorded on the access control system, where all access activity is monitored and reported - this information is archived for audit purposes.

Access passes must be visible at all times, to facilitate visual checks. Redcentric personnel are responsible for carrying out such checks and ensuring that no visitor is in Redcentric areas without a pass.

Failure to display a pass will result in the individual being escorted from the area immediately and potentially being escorted offsite by Redcentric personnel.

Visitors may only access viewing galleries when escorted by Redcentric personnel, with prior agreement. Private hosting suites can only be accessed by appropriately screened and authorised Redcentric personnel and the customer.

Redcentric & customer engineers are only permitted entry into Redcentric private hosting suites with prior authorisation and with an escort provided by Redcentric personnel, unless previous authorisation has been obtained from the customer for unescorted access.

Private hosting suite customer representatives, with their own permanent access pass can access their own areas without prior warning to Redcentric.

At no time should customer representatives with a permanent access pass attempt to allow access to any non-cardholders without a prior access request being raised.

Whilst on site, if the visitor is in any doubt concerning access to any Redcentric areas, they should seek immediate advice from Redcentric Management or the Facilities department. While advice is being sought, it is the responsibility of Redcentric personnel to prevent any further access or action being performed by the visitor.

Records of all access, including appropriate signatures and associated access privileges granted will be maintained for a period of two years after termination of privileges.

Individual Redcentric personnel and customers with granted access authority are responsible for maintaining the security and confidentiality of data or equipment in their possession at all times. Individuals must report to Redcentric any known or suspected breach of security.

3.6 Mobile Phones

Mobile phones are permitted within the Data Centres, however, Redcentric reserve the right to confiscate such devices if the user is observed taking photographs or recording video footage.

3.7 Video streaming & recording

Video streaming is not permitted whilst walking and or moving throughout any of Redcentric Data Centres.

Redcentric acknowledge that video calls may need to be conducted onsite, but video calls must be conducted

- Within customer's own private suite
- Directly outside their own cabinets (if they are trying to troubleshoot a fault)
- Common refreshment areas

Redcentric reserve the right to request immediate termination of any video call should, and request proof that any video footage has been deleted.

4 Engineering Visit Requirements

4.1 Risk Assessment and Method Statements

Where a Risk Assessment is required, this must detail the scope of the planned work and also identify any associated risks, explaining how these will be mitigated.

The Method Statement if required, must detail how the work is to be conducted, in addition to safety procedures to be followed during the work.

Whilst work is being undertaken and floor tiles removed, Redcentric Facilities personnel will take control of the area, providing signage and marshalling the area.

4.2 Emergency works

In cases where work needs to be completed as an emergency and the requestor cannot provide the required documentation in advance, this can be achieved with Facilities department approval.

The visitor must attend site and undertake a site induction with Facilities personnel and the Risk Assessment and Method Statement documentation must be completed by the visitor following the induction and approved by a member of the Facilities department before the work can commence.

If the visitor does not possess templates for the required documentation, these can be provided by Redcentric Facilities personnel.

It is the responsibility of the visitor to ensure that all forms are completed correctly.

4.3 Completion of works

Once the work has been completed, Redcentric personnel will check the area prior to the visitor leaving site, to ensure that the area is safe, and that all equipment associated with the work has been removed.

Redcentric personnel will also confirm that any equipment installed/removed, matches that recorded within the interaction record.

5 Security

To maintain security of the organisation's data centre and office environments, Redcentric maintains strict access controls and checks at all times.

5.1 Visitors

Guidance for on-site visitors is available at Redcentric reception.

All visitors are required to report any security issues or concerns immediately to the Redcentric facilities or support contact.

5.2 Employees

All employees and contractors carrying out work on behalf of Redcentric must report any security incident, event or weakness to ISO@redcentricplc.com as per the formal Security Incident Management Policy located on the company SharePoint (available to visitors on request).

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED