Datum

MCR 1: Data centre security

At Datum, we take physical and logical security extremely seriously, which is why we've implemented some of the most advanced and robust security measures seen at any building in the country.

www.datum.co.uk

Security at MCR 1

From perimeter security to secure access procedures, everything at MCR1 is designed to identify, prevent and then manage any potential issue with minimum disruption and the ultimate response.

A major consideration for us, is that our authorised colocation customers require 24/7 access. We manage this access through the use and integration of advanced electronic controls and intelligent identification systems, with extensive audit trails and live monitoring of all security systems.

Certified security at Datum MCR 1

bsi ISO/IEC 27001 Information Security Management CERTIFIED
IS590824

PASF
Police Approved Secure Facility

PCI DSS COMPLIANT

Physical security measures

On-site SOC (Security Operations Centre)

MCR1 is one of the only data centres in the UK to benefit from an on-site BS5979, NSI Gold Approved Alarm Receiving Centre, offering live monitoring of all security systems and direct links to police control rooms. Benefits of the SOC include:

- Located within a BS5979 certified secure 'bunker', with all security personnel protected from potential intruders.
- Man-trap secure entry into the SOC, with vibration detection protecting the re-enforced shell from potential attack.
- 24/7 BS7858 vetted, SIA approved security staff.
- CCTV monitoring to BS8418 standards.
- Audio challenge systems to challenge unwanted visitors remotely.
- Separate data centre, fibre and power supplies to ensure autonomous continuation and security provision in the event of a main data centre issue.
- Ability to interact remotely with all building doors and entry systems.

Perimeter security

Security starts at the perimeter of the building, with all areas protected, secured and monitored by a range of features — these include:

- Full height security fencing surrounding the full building compound.
- Dedicated entry/exit high speed security gates.
- ANPR vehicle identification systems to recognise authorised visitors and allow automatic entry.
- Virtual trip-wire technology to identify intruders.
- Full CCTV coverage of all external areas.
- Audio challenge PA systems.
- Thermal detection for the accurate identification of unwanted or unexpected visitors.

Main building entrance

Once inside the building, a range of high security processes and procedures work to protect the data halls against unauthorised access.

- High security entrance door with anti-tailgating technology, volumetric detection and access control.
- Dedicated delivery air-locks with interlocking electronic security doors, remotely controlled by on-site security personnel.
- Monitored and police linked Grade 3 intruder alarm system to all external doors and entry points.
- Visitor ID checking via high-grade CCTV cameras prior to access being granted.
- Tamper detection and alarms to all entrances.
- Access controlled turnstiles within reception for additional security.

Data centre entrances

Our data halls are protected by 4-factor access control for ultimate peace of mind.

- Re-enforced and alarmed high security air-locks.
- 4-factor access control — access card, PIN number, volumetric and biometric checks:
    - Access card and PIN number unique to user.
    - Volumetric check ensures only single visitors pass through air-locks.
    - Biometric (iris) checks validate identity of user.
- All checks must be validated and passed before entry granted to data halls.
- Failed attempts immediately notified to security.
- Full audit logs retained for all access attempts.

Data hall security

- Extensive monitored CCTV.
- PIR sensors that alarm on unexpected motion detection.
- Combination locks on all rack doors.
- Additional security features available to individual racks.

Security access prodedures

Client portal

All clients are provided with access to a secure online portal to give full control of users that:

- Have access to the building and are allocated access cards.
- Are added to the building ANPR system for automatic gate entry.
- Are able to access designated areas where they have rack space.
- Are able to raise support tickets.
- Require immediate disablement.

To be allocated an access card and enrolled for data centre access, users must attend an enrolment appointment where their ID is checked and their details stored on our system. Enrolled users will also have their iris scanned and their profile stored on the biometric systems.

Access management

Authorised users on Datum's client portal access list are able to access the data centre 24/7, with only out-of-hours visits requiring prior notification.

Engineers and authorised third parties can access the facility as long as they can provide valid photo-ID on arrival and they have been pre-booked via the online portal by an authorised Datum portal user.

Datum: unrivalled data centre security

Our multi-layered approach to data centre security provides our clients with confidence in our ability to deliver a robust service. It also has a strong impact on our clients' commitments to their customers and helps to ensure that our facilities will meet and exceed the expectations of an enterprise class data centre facility.

This security resilience has attracted clients to Datum from across IT and cyber security, defence, construction, finance and the public sector. Our security approach is unrivalled and processes across our facilities have been designed to meet the requirements of industry-recognised certifications including ISO 27001, PCI DSS, BS5979, NSI Gold and PASF.

Book now

Take advantage of one of our no-obligation data centre tours and see our first class security processes for yourself — contact us to book a data centre tour for any of our UK facilities:

www.datum.co.uk
info@datum.co.uk
0161 498 1200

Datum

Contact us

Datum Datacentres Limited
Delta House, Wavell Road,
Manchester, M22 5QZ

UK 0161 498 1200