



Information Security Program

Data Center Physical Access Policy

Document Name:	INFOSEC_DCPHYSACCESS_POLICY_2026.1
Version:	2026.1
Date of version:	December 3, 2025
Reference:	ISO27002 11 Physical and Environmental Security
Created by:	M. Schuetter
Approved by:	R. Dobson
Classification level:	Confidential

Change History

Date	Version	Created By	Description of change	Approved By
2016-10-21	1.0	M. Schuetter	Initial document authorized by management	J. Vollmer
2016-12-16	2017.1	M. Schuetter	Modified version control and document authorization sections.	J. Vollmer
2017-02-10	2017.2	M. Schuetter	Added clarification to visitor access requirements	J. Vollmer
2017-09-25	2017.3	M. Schuetter	Modified customer review frequency to match our expectations	J. Vollmer
2017-11-03	2018.1	M. Schuetter	Annual review and minor syntax changes	J. Vollmer
2018-11-16	2019.1	M. Schuetter	Annual review and minor syntax changes	D. Burns
2019-11-15	2020.1	M. Schuetter	Annual review	D. Burns
2020-11-20	2021.1	M. Schuetter	Annual review	R. Dobson
2021-11-19	2022.1	M. Schuetter	Annual review	R. Dobson
2022-12-16	2023.1	M. Schuetter	Annual review	R. Dobson
2023-12-14	2024.1	M. Schuetter	Annual review	R. Dobson
2024-12-09	2025.1	M. Schuetter	Annual review	R. Dobson
2025-12-03	2026.1	D. Verdon	Annual review	D. Burns

TABLE OF CONTENTS

1. Introduction.....4

2. Scope 4

3. Data Center Physical Access Policies 4

 3.1. Defined Roles..... 4

 3.2. Access to the Data Center..... 5

 3.3. Access Authorization..... 5

 3.4. Visitor Procedures..... 6

 3.5. Audit Procedures 6

4. Validity and Document Management.....6

5. Reference Documents.....7

1. Introduction

Encore Technologies (“Encore” or the “Company”), as part of the Information Security Program (the “Program”), has the responsibility to control physical access to its Data Center. This policy outlines the Program’s requirements for administering and restricting physical access to the facility.

The purpose of this policy is to outline the high-level controls, designed and implemented by the Program, to ensure required physical access to the Data Centers, customer cages and cabinets, is appropriately granted and maintained.

2. Scope

This Policy applies to all personnel that require access to the following Encore Data Centers to perform appropriate business/IT functions.

- 4620 Welsey Avenue, Cincinnati, OH 45212
- 11515 Grooms Rd, Cincinnati, OH 45242
- 9333 N Springboro Pike, Miamisburg, OH 45342
- 8700 Governors Hill Dr, Cincinnati, OH 45249

3. Data Center Physical Access Policies

3.1. Defined Roles

The following defined roles are referenced throughout this Policy.

- 3.1.1. **Data Center Employee:** Encore employees and/or its designees who primarily work at the Data Center.
- 3.1.2. **Data Center Manager:** Any Encore employee that is responsible for the overall supervision and management of the Data Center.
- 3.1.3. **Authorized Encore Staff:** Encore employees who are authorized to gain access to the Data Center but who do not primarily work at the Data Center.
- 3.1.4. **Authorized Vendor:** All Encore/Data Center/Customer vendors who, through contractual arrangement and appropriate approvals, have access to the Data Center.
- 3.1.5. **Authorized Designated Contact:** A Customer representative who is authorized to approve Data Center access to other Customer employees.
- 3.1.6. **Authorized Customer Staff:** All customer employees who are authorized by their associated Authorized Designated Contact to gain access to their customer cages, cabinets and equipment within the Data Center.
- 3.1.7. **Visitors:** All other personnel who may occasionally visit the Data Center but are not authorized to be in the Data Center without escort.

3.2. Access to the Data Center

All personnel authorized for unescorted Data Center access will abide by the following set of policies:

- 3.2.1. All personnel who access the Data Center must have proper authorization (see section 3.3).
- 3.2.2. All authorized vendors and customer staff will exchange a driver's license or government issued photo ID to receive a Data Center identification badge. Data Center identification badges will be returned when exiting the Data Center.
- 3.2.3. All personnel must wear a valid Data Center identification badge at all times.
- 3.2.4. All non-Data Center and Encore employees must use the then-in-use physical access controls to enter and exit the Data Center, as well as when gaining access to their associated cages and cabinets.
- 3.2.5. Authorized personnel will have access to the Data Center at any time.
- 3.2.6. Visitors to the Data Center must adhere to the visitors' procedures (see section 3.4).
- 3.2.7. Authorizations will be reviewed and verified based on the audit procedures on a regular basis (see section 3.5).
- 3.2.8. Access to the Data Center will be monitored by Data Center employees through video surveillance cameras. Video files will be maintained in accordance with Encore's **Data Center Video Surveillance Policy**.
- 3.2.9. Encore may restrict access to any shared work area within the Data Center at any time.

3.3. Access Authorization

Access is granted to the Data Center as follows:

- 3.3.1. Data Center access will only be approved for individuals who are responsible for installation, monitoring and/or maintenance of equipment housed in the Data Center.
- 3.3.2. Data Center and authorized Encore employees must be pre-approved by Encore management for unescorted access.
- 3.3.3. Vendor access must be pre-approved by authorized personnel.
- 3.3.4. The Access Authorization process is as follows:
 - 1. Authorization requests must be approved by an Authorized Designated Contact of the Company.
 - 2. The Authorized Designated Contact may require and formally document escort restrictions for any authorized personnel.
 - 3. If approved, the authorized customer staff member or vendor will be added to the authorization database, and the authorization request will be kept on file.

4. Personnel authorized to access the Data Center will be required to enroll into a biometric or other system as part of the physical access control infrastructure and have their photograph taken for badging and placed into the authorization database.

3.4. Visitor Procedures

All visitors to the Data Center must adhere to the following procedures:

- 3.4.1. Visitor authorization requests must be approved by an authorized designated contact.
- 3.4.2. Visitors must be accompanied by either a Data Center employee or other authorized staff member at all times. Exceptions to this policy must have the approval of the Data Center manager.
- 3.4.3. Visits must be scheduled through the Data Center manager at least 2 business days in advance. Unscheduled visitors may be turned away.
- 3.4.4. All visitors must show a valid government issued photo ID and sign the Visitor Log before escorted entrance is allowed.

3.5. Audit Procedures

To ensure the authorized access list for each Customer remains current, the following activities will be performed:

- 3.5.1. The Data Center manager will send a list of authorized staff and authorized vendors ("authorized access list") to the appropriate Authorized Designated Contact for review and verification every 12 months.
- 3.5.2. Each Authorized Designated Contact will review and update the authorized access list of authorized staff/vendors and return it to the Data Center manager within 5 business days.
- 3.5.3. Failure to return the authorized access list will result in revocation of access privileges for previously authorized staff/vendors until the authorized access list is returned.
- 3.5.4. The Data Center manager will modify access controls within 5 business days of receipt.

4. Validity and Document Management

This policy is authored by Information Security management and authorized by Encore Corporate Leadership. On an annual basis, the Information Security Program documentation will be reviewed followed by formal approval by Encore Corporate Leadership. If material updates or modifications are made at any time to these documents, changes must be presented and approved by Encore Corporate Leadership before authorization.

5. Reference Documents

Type of Document	Version when Published	Document Name
Policy	2026.1	Information Security Policy
Policy	2026.1	Data Center Acceptable Use Policy
Policy	2026.1	Data Center Video Surveillance Policy