



Information Security Program

Data Center Acceptable Use Policy

Document Name:	INFOSEC_DCACCEPTUSE_POLICY_2026.1
Version:	2026.1
Date of version:	December 3, 2025
Reference:	ISO27002 7 Human Resource Security
Created by:	M. Schuetter
Approved by:	D. Burns
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 a formal incident reporting section	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
2020-11-30	2021.1	M. Schuetter	Annual review	R. Dobson
2021-11-19	2022.1	M. Schuetter	Annual review with modification about customer power	R. Dobson
2022-12-20	2023.1	M. Schuetter	Annual review	D. Burns
2023-12-14	2024.1	M. Schuetter	Annual review	D. Burns
2024-12-09	2025.1	M. Schuetter	Annual review	D. Burns
2025-12-03	2026.1	D. Verdon	Annual review	D. Burns

TABLE OF CONTENTS

1. Introduction.....4

2. Scope 4

3. Data Center Acceptable Use.....4

 3.1. Data Center Access and Notifications 4

 3.2. Personnel Conduct..... 5

 3.3. Online Conduct 6

 3.4. Third-Party Actions 6

 3.5. Power Usage 7

 3.6. Equipment and Connections 7

 3.7. Shipping 8

 3.8. Maintenance..... 9

 3.9. Incident Reporting 9

4. Validity and Document Management.....9

5. Reference Documents.....9

1. Introduction

Encore Technologies (“Encore” or the “Company”), through the implementation of its Information Security Program, has the responsibility to protect the Company, employees, and customers from damaging and/or illegal actions carried out through the use of its facilities and IT resources.

The purpose of this policy is to outline the acceptable use of facility, computer and network resources within the Encore Data Centers. These requirements are designed to protect the Company and its customers from human and IT-related risks. It is the responsibility of every user to read, understand, and follow this policy.

2. Scope

This Policy applies to all personnel who access the following Encore Data Centers:

- 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 Acceptable Use

The following sections outline general provisions governing the use of Encore IT systems and the ownership of data contained therein.

3.1. Data Center Access and Notifications

- 3.1.1. The Customer will designate one or more persons with associated contact information whom Encore may contact at any time (“authorized designated contact”). The authorized designated contacts must be readily available and familiar with the Customer’s use of the Data Center facility and Customer equipment.
- 3.1.2. Only Customer personnel on the Authorized Access List may access the Data Center for business purposes. Please refer to the **Data Center Physical Access Policy** for more information regarding access.
- 3.1.3. The Customer will only access that portion of the Data Center made available by Encore to the Customer for the placement of its equipment and usage of Data Center Services.
- 3.1.4. The Customer accepts full responsibility for the actions of its authorized personnel, accompanying persons and other associated entities and must ensure they do not take any actions that the Customer is prohibited from taking under these policies.
- 3.1.5. Encore reserves the right to exclude or expel Customer personnel who, in Encore’s judgment, pose a risk to persons or property in the Data Center.

- 3.1.6. Encore reserves the right to suspend a Customer's operations and/or access in and around the facility, if there arises a hazardous condition or emergency situation. Encore will notify the Customer's authorized designated contact of such conditions as soon as reasonably possible.

3.2. Personnel Conduct

The Customer will abide by all security and safety measures established by Encore. The Customer and its associated personnel will ensure:

- 3.2.1. The Customer will not misuse or abuse any Encore property or equipment or third-party equipment.
- 3.2.2. The Customer will not make any unauthorized use of or interfere with any property or equipment of Encore or any other Encore customer.
- 3.2.3. The Customer will not harass any individual, including Encore personnel and representatives of other Encore customers.
- 3.2.4. The Customer will not engage in any activity that is in violation of the law or aids or assists any criminal activity while on Encore property or in connection with Encore and its associated facilities.
- 3.2.5. The Customer will not obstruct exit routes, pathways, driveways, entrances, hallways, or stairs, in and around the Data Center or other Encore facilities.
- 3.2.6. The Customer will not place furniture within the Data Center except where permitted by the Data Center manager.
- 3.2.7. The Customer will not install surveillance equipment of any kind without prior Data Center manager consent. Encore reserves the right to have Customer remove or relocate surveillance equipment if it impedes or interferes with the security and/or privacy of others.
- 3.2.8. The Customer will not bring any prohibited materials into the Data Center including:
- Food and drink
 - Tobacco, vaping or other related products
 - Hazardous or combustible materials
 - Alcohol, illegal drugs or other intoxicants
 - Electro-magnetic devices that could interfere with computer and telecommunications equipment
 - Explosive or radioactive materials
 - Photographic equipment of any kind
 - Weapons of any kind
- 3.2.9. The Customer will not generate, transport, store or dispose of any hazardous materials within or around Encore properties.

- 3.2.10. The Customer will maintain its Customer cages/cabinet(s) in an orderly and clean manner and deposit litter in designated receptacles or in appropriate locations outside the Data Center.

3.3. Online Conduct

The Customer acknowledges that Encore does not control the content of the information passing through the Customer's environment within the Data Center and that it is the sole responsibility of Customer to ensure that the information it and its users transmit and receive complies with all applicable laws and regulations and this Acceptable Use Policy.

The Customer will not permit any persons using Customer's environment, including its applications, systems and network infrastructure, to do any of the following:

- 3.3.1. The Customer will not send unsolicited commercial messages or communications in violation of applicable law or governmental regulation.
- 3.3.2. The Customer will not engage in any activities or actions that infringe or misappropriate the intellectual property rights of others.
- 3.3.3. The Customer will not engage in any activities or actions that would violate the personal privacy rights of others, including, but not limited to, collecting and distributing information about Internet users without their permission.
- 3.3.4. The Customer will not send, post or host harassing, abusive, libelous or obscene materials or assist in any similar activities.
- 3.3.5. The Customer will not intentionally omit, delete, forge or misrepresent transmission information, including headers, return mailing and Internet protocol addresses.
- 3.3.6. The Customer will not use the Encore connectivity services for any illegal purposes, in violation of any applicable laws or regulations.
- 3.3.7. The Customer will not assist or permit any persons in engaging in any of the activities described above.

3.4. Third-Party Actions

From time to time, third parties may cause situations in which customers leveraging Encore shared Internet services is degraded or disrupted.

- 3.4.1. Encore cannot guarantee that such third-party actions will not occur and disclaims any liability of damages related to or resulting from such events.
- 3.4.2. Encore reserves the right to suspend without liability the Customer's services that may be interfering with or disrupting the Data Center and/or its other customers.

- 3.4.3. Encore will make commercially reasonable efforts to notify Customer of any such harmful use prior to suspending Customer's service.
- 3.4.4. Encore will restore service when it reasonably deems there is no further threat of harm to the Encore network or its operation or the operations of its other customers.

3.5. Power Usage

The following policies apply to all equipment and connections housed within the Data Center:

- 3.5.1. All installations of cabinet PDUs to the installed circuits must be done by an Encore authorized employee.
- 3.5.2. The Customer will not connect a power circuit to a cabinet PDU except the one specified by Encore.
- 3.5.3. The Customer will not consume power beyond the limit of any power circuit.
- 3.5.4. The Customer will not use circuit splitters on any Encore-provided power circuit.
- 3.5.5. The Customer will not use non-Encore provided UPS systems without Encore approval.
- 3.5.6. The Customer will not use non-Encore provided 48v DC rectifiers without Encore approval.
- 3.5.7. The Customer will not use VRLA (valve-regulated lead-acid) batteries within the Data Center, unless manufacturer installed and an integrated part of equipment that received a formal exception from the Data Center manager.

3.6. Equipment and Connections

The following policies apply to all equipment and connections housed within the Data Center:

- 3.6.1. The Customer is fully responsible for using its Customer cages/cabinets and associated Customer equipment in a safe and lawful manner.
- 3.6.2. The Customer will ensure that all Customer equipment is installed, operated and maintained in compliance with Encore and manufacturer specifications including power outlet, power consumption and clearance requirements.
- 3.6.3. The Customer will ensure that all Customer cabling remains within the Customer Cabinet(s) and abide by Encore specifications.
- 3.6.4. All Customer equipment must be clearly labeled with Customer name and component ID. All cross connects will be labeled with Customer name and starting and ending point for the cross connect.
- 3.6.5. The Customer is responsible for obtaining telecommunications services as needed from the carrier of its choice.

- 3.6.6. Customer equipment will not interfere with Encore Data Center power and air handling infrastructure.
- 3.6.7. The Customer will not store any paper/cardboard products or other combustible materials of any kind in Customer cages or cabinets.
- 3.6.8. Encore may require the Customer to remove any Customer equipment that it considers to be unsafe and/or interferes with the operations of the Data Center, Encore or another customer.
- 3.6.9. Encore will not interact with Customer equipment except in the case of emergency or where explicitly approved by authorized Customer staff.
- 3.6.10. The Customer is responsible for any loss, theft or damage to Customer equipment left unattended and outside of Customer cabinets.
- 3.6.11. Encore is not responsible for any electronic interference to the Customer's use of wireless communications equipment.
- 3.6.12. Encore may access Customer cages and/or cabinets during an emergency or to perform authorized services for or on behalf of the Customer.

3.7. Shipping

The following policies apply to shipping and receiving within the Data Center on behalf of the Customer:

- 3.7.1. The Customer will adhere to all shipping and receiving procedures in effect at the Data Center and is responsible for all charges related to Customer equipment shipping.
- 3.7.2. The Customer will ensure all shipments are clearly labeled with Customer name/identifier. The Customer will not use Encore as the recipient of any Customer deliveries to the Data Center.
- 3.7.3. Shipments not properly identified will be rejected by Data Center employees. Additionally, shipments containing liquids, combustibles, and any hazardous material are prohibited and will not be accepted at any time.
- 3.7.4. Encore may visually/physically inspect all shipments to and from the Data Center. Upon receipt, Encore may record serial numbers for shipped Customer Equipment.
- 3.7.5. The Customer is responsible for moving shipments from Shipping/Receiving area to the Customer cage/cabinet(s).
- 3.7.6. Encore is not responsible or liable for missing or damage to Customer Equipment due to faulty packaging or shipment.

3.8. Maintenance

- 3.8.1. Encore will conduct routine scheduled maintenance of its Data Center and Data Center Services as are reasonably required to maintain the Facilities.
- 3.8.2. In the event a mission critical maintenance situation arises, Encore may be required to perform emergency maintenance at any time.
- 3.8.3. Customer agrees to cooperate with Encore during the scheduled and emergency maintenance periods.

3.9. Incident Reporting

- 3.9.1. The Customer will notify Encore of any damage or risk of damage to the Data Center, or to Data Center, Encore or other customer equipment.
- 3.9.2. All personnel who access the Data Center must report unusual or suspect activity to the onsite physical security immediately.
- 3.9.3. Other cyber security concerns must be reported to the Encore Information Security Program at security@encore.tech.

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 Physical Access Policy