



Information Security Program

Data Center Video Surveillance Policy

Document Name:	INFOSEC_DCVIDEOSURVEILLANCE_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
2017-01-13	2017.1	M. Schuetter	Initial document authorized by management	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 and minor syntax changes	D. Burns
2020-11-30	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. Video Surveillance Policy 4

 3.1. Video Surveillance Usage 4

 3.2. Video Surveillance Management 4

 3.3. Video Surveillance Monitoring..... 5

 3.4. Video Surveillance Recording..... 5

 3.5. Video Surveillance Limitations 6

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

5. Reference Documents.....6

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 within its facilities or through the use of its IT resources.

The purpose of this policy is to outline the use of video surveillance throughout Encore Data Center facilities in order to support this effort.

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. Video Surveillance Policy

This Video Surveillance Policy provides guidance regarding the use of video surveillance systems.

3.1. Video Surveillance Usage

- 3.2.1 Video surveillance systems are primarily used to record access at building entrances, lobbies and controlled areas of the premises. Video surveillance cameras are also used to provide surveillance of the exterior of the building, and potentially parking lots and surrounding streets.
- 3.2.2 Video surveillance cameras are generally not used to observe employee work areas with the exception of data center raised floor aisles and are never used in areas where employees would have an expectation of privacy, such as restrooms or locker rooms.
- 3.2.3 The primary purpose of the video surveillance system is to support the after-the-fact investigation of crimes committed against the Company as well as unprofessional behavior. The system may also be used to assist in the investigation of certain types of occupational health and safety violations.
- 3.2.4 The video surveillance system is not intended to be used as a method of tracking the work habits or productivity of individual employees.
- 3.2.5 Use of video surveillance systems will be disclosed to the public.
- 3.2.6 The information produced by the system will be safeguarded in accordance with local laws and fair information practices.

3.2. Video Surveillance Management

- 3.2.7 Facilities Management is responsible for the management of all video surveillance systems used at the Company.

- 3.2.8 Other corporate departments or customers shall not install video surveillance systems without the knowledge and approval of Facilities Management.
- 3.2.9 In particular, the use of covert camera systems must first be approved by both the Encore Corporate Leadership with consultation from legal counsel.

3.3. Video Surveillance Monitoring

- 3.3.1 The video surveillance systems will be monitored by Facilities Management's Physical Security.
- 3.3.2 The video surveillance systems are capable of being monitored from the Physical Security Desk located at the main entrance lobby and remotely by other authorized personnel.
- 3.3.3 Security officers generally view video surveillance cameras on a periodic basis or in response to a specific incident. Because of the many responsibilities of the officer(s) at the Security Desk, the video surveillance system may not be monitored on a continuous basis.

3.4. Video Surveillance Recording

- 3.4.1 All video surveillance cameras are capable of being recorded continuously or triggered based on activity within its field of view by a digital video recording system.
- 3.4.2 Recorded video is generally stored for a period of thirty days for outside footage and ninety days for internal footage.
- 3.4.3 Recorded video is used exclusively for the investigation of security and safety incidents and not for other purposes.
- 3.4.4 Facilities Management is responsible for the management of the video surveillance system and has exclusive control of the release of video recordings produced by this system.
- 3.4.5 Recorded video is not made directly available to Encore employees, building tenants, or the general public. In the event that a security incident occurs, employees should report the incident to the Facilities Manager. If the event occurred in an area where video surveillance coverage is available, the Facilities Manager will review the recorded video and make a determination if any video relevant to the incident is available. This video will be used by the Facilities Manager to investigate and resolve the reported security or safety incident.
- 3.4.6 Requests to provide video recordings directly to non-employees (such as tenants, neighbors, or members of the general public) will not be accommodated.
- 3.4.7 Any video associated with a specific security or safety incident or event is generally converted into a permanent video clip and stored for the duration of the investigation.
- 3.4.8 Video clips which could become evidence in civil or criminal proceedings are kept indefinitely unless other direction is given by Encore legal counsel.
- 3.4.9 Requests by law enforcement:
 - a. If a crime has been committed, non-employees should be encouraged to report it to the police.

- b. If it is believed that recorded video from Encore would assist in the investigation of this crime, the police should be told to contact the Encore Facilities Manager.
- c. If relevant video is available, a permanent video clip of the incident will be produced and made available to law enforcement.
- d. All requests for video recordings by law enforcement agencies shall be coordinated through Encore Corporate Leadership with assistance from legal counsel as needed.

3.5. Video Surveillance Limitations

- 3.5.1 Employees should be aware that a security officer is not watching most cameras most of the time and employees should not have an expectation that they are under continuous surveillance when they are in the range of a camera.
- 3.5.2 Employees should also be aware that the video surveillance system has cameras that cover only a small fraction of the total campus, and even when camera coverage exists, it may not provide the level of detail necessary to spot suspicious activity or identify criminals.

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 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
Policy	2026.1	Physical and Environmental Security Policy