

 <p>University of CINCINNATI</p> <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Students/ Affiliates/Guests</p>	<p><i>Policy Title:</i> Data Center Visitor</p> <p>Effective Date: 09/03/2021</p> <p>Prior Effective Date: 10/25/2017</p>	<p><i>Policy Number:</i> 9.1.25</p> <p>Policy Owner: VP & CIO, UC Information Technologies</p> <p>Responsible Office(s): Office of Information Security</p>
--	--	--

Background

The purpose of this policy is to define the physical security measures that must be followed when hosting any visitor to data center facility. It is designed to provide procedures of how visits must be carried out, ensuring control procedures are applied as preventive measures against any human threat to resources and sensitive information housed in the data center.

Policy

- Anyone accessing the data center must sign the logbook at the entrance to the data center. These logbooks will be retained by the data centers for a period of three years. Logs must be reviewed quarterly for unauthorized access.
- A list of data center authorized individuals must be maintained. Anyone not on the authorized individuals list must be treated as a data center visitor. This includes university personnel and third-party vendors regardless of the reason for the visit. The authorized individuals list must be reviewed bi-annually.
- The data center must have authorized staff members physically present as an escort to monitor the visitors in the data center. This monitoring must be in effect throughout the duration of the visit.
- Physical contact to data center technology and infrastructure components by any unauthorized individual, is strictly prohibited. This prohibition against physical contact includes unauthorized university employees and unauthorized third-party vendors, regardless of the reason for the visit.
- There must be a ratio of one authorized staff member in attendance for every five visitors at the time of the visit.

- The taking of pictures, videos, or the recording of data is strictly prohibited.
- To be eligible to enter the data center, visitors must be citizens of the United States or must be permanent resident aliens green card holders. Non-immigrant foreign nationals are not permitted to enter the data center for any reason.

Visitor access to the State of Ohio Computer Center (SOCC) is governed by this policy and the contractual agreement in place.

Contact Information

Office of Information Security

513-558-ISEC (4732)

infosec@uc.edu

Definitions

Data Custodian: computer system administrators responsible for the operation and management of systems and servers which store or provide access to institutional data.

Data Steward: university employees who have direct operational-level responsibility for information management.

Data Trustee: university administrators at the vice-presidential level who bear the ultimate responsibility for ensuring the protection of the data stored by those in their reporting area.

Related Links

[Data Governance & Classification Policy](#)

[Data Center Visitor Procedure](#)