Background

The purpose of this policy is to define the physical security measures that must be followed when hosting any visitor to the IT@UC 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. All data center facilities that store or process PCI (Payment Card Industry) data or export control data must adhere to this policy. This includes IT@UC and Unit IT data center facilities. It is the responsibility of Data Trustees and Data Stewards to notify the corresponding Data Custodians of the presence of PCI or export control data.

Policy

- All visitors to the data center must sign the log book at the entrance to the data center. These log books will be retained by the data centers for a period of three years.
- 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.
- Authorized staff members must be aware that any physical contact to the computer systems and its components by any unauthorized individual, regardless of the visitor being either a university employee or outside entity, is strictly prohibited.
- 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’). 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 the contractual agreement in place.
Contact Information

IT@UC 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

History

Issued: 01/04/2008
Revised: 01/04/2013
Reviewed: 03/04/2016
Revised: 07/20/2016