Tier 1 Control Standards (State-Wide)

IOT Physical Security

Standard ID
IOT-CS2-SEC-100

Published Date
5/21/2007

Effective Date
5/21/2007

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
06.0 Access Control (PR.AC)
06.2 PR.AC-2
06.2.1 Physical Access

Purpose
The purpose of the IOT Physical Access Policy is to establish guidelines for physical access to IOT facilities and to IU Data Center (DR Site). The scope of this practice extends to all IOT owned and operated facilities in order to protect information resources on behalf of the State.

Scope
IOT

Statement
IOT will secure and limit access to the data center, communication closets, and equipment inventory storage. Access to IOT office space will be secured during non-business hours (4:30 pm to 7:00am). Access during business hours will be restricted by badge access or access through the main IOT entrance. The following apply:

- The IOT Badge Access Standard will be followed to ensure proper access for IOT personnel and contractors.
- Managers are responsible for specifying the minimum access privileges necessary to complete job duties. Managers shall review facilities access for their employees and any contractors under their supervision and a recurring basis for appropriateness.
- Managers and/or employees are responsible for promptly notifying appropriate personnel when access to IOT facilities has been terminated or suspended.
- Access to data processing and communications facilities are subject to specific use guidelines established by the IOT manager of the facility (see below for additional information regarding access to IOT facilities). All visitors to these areas will be aware of access requirements and limitations. Unauthorized access or activities subject employees and contractors to disciplinary action up to and including dismissal or loss of contract and criminal prosecution when appropriate.
- Access to the facilities outside of business hours will be controlled through proper badge access. Access to the Indiana government center for evenings and weekend hours must be requested through Department of Administration form 52044.

IOT Office Access

- Normal Hours (7:00 a.m. – 4:30 p.m.)
- IOT workforce (employees and contractors)
Access to IOT offices shall be controlled electronically by a Card Access System. IOT employees and contractors are granted access only to those facilities and resources needed to perform their duties.

Managers shall request new or changed access for employees and contractors via email or in person to a member of the Security Team.

Upon termination it is the responsibility of the employee or contractor manager to immediately have access rights to facilities removed. This is to be accomplished via an email unless there is an elevated security concern. In such cases, security team shall be contacted directly to ensure timely removal of access rights.

Any employee losing an access card is to immediately contact the Security Team to report and request that card privileges of the lost badge will be eliminated.

- **Visitors (includes delivery and pickup)**
  - Visitors without a State of Indiana security badge accessing IOT work areas are to be escorted.
  - Visitors shall report to the front desk and await escort into the working area. (Delivery personnel i.e. FedEx, UPS, etc. are managed by IDOA.)
  - State employees (non-IOT) or contractors may travel unescorted through IOT work areas as long as they have and display a valid State of Indiana security badge.
  - IOT employees will not leave un-badged state employees or vendors in work areas without an escort.

- **Service personnel**
  - Authorized service personnel (electricians, phone technicians, plumbers, property management, etc.) shall check in at the front desk. If the service is approved, IOT employees do not need to escort the service provider throughout their work.

- **After Hours/Weekends/Holidays Access**
  - IOT workforce (employees and contractors)
    - Requests for access to the North/South MDF, communication closets, and data center access are to be first approved according to the IOT Badge Access Standard.
    - Staff must follow the rules of conduct established by the owner for visitation and use of the facility.
    - Upon termination it is the responsibility of the employee or contractor manager to immediately have access rights to facilities removed.
  - **Visitors (includes delivery and pickup)**
    - Visitation to IOT work areas after normal business hours is to be scheduled with an IOT employee or contractor, coordinated with the employee or contractor, and escorted as required by the nature of the work and business relationship. There are to be no unescorted visitors in IOT work areas after hours without appropriate authorization and/or supervision.
    - Visitors shall gain access through preplanned means and abide by all Government Center entry requirements.
    - Visitors shall limit their visit to authorized locations and leave promptly upon completion of their work.

- **Service personnel**
  - Accommodations shall be made by responsible parties for the entry of authorized service personnel (electricians, phone technicians, plumbers, property management, etc.) conducting assignments after normal business hours.

**Indiana Government Center North/South MDF, Communication Closets, and Data Center Access**

Access to key data processing and communications facilities are subject to specific use guidelines established by the business owner of the service housed in the facility. All visitors to these areas shall be aware of access requirements and limitations. Unauthorized access or activities subject employees and contractors to disciplinary action up to and including dismissal or loss of contract and criminal prosecution when appropriate.

- **Normal Hours (7:00 a.m. – 4:30 p.m.)**
- **IOT workforce (employees and contractors)**
  - Requests for access to the North/South MDF, communication closets, and data center access are to be first approved according to the IOT Badge Access Standard.
  - Staff must follow the rules of conduct established by the owner for visitation and use of the facility.
  - Upon termination it is the responsibility of the employee or contractor manager to immediately have access rights to facilities removed.
- **All others (visitors, service)**
  - Visitation to the MDF, communications closets, and data center by non-workforce members is only permitted with authorization from the Network Services or Data Center manager or designees per the IOT Badge Access Standard. Escort requirements and rules of conduct established by facilities owners are to always be obeyed.

**UITS Facilities Building and Data Center, 2737 East Tenth Street, Bloomington, Indiana 47408-2671**

Any State employee or contractor requiring access to UITS Data Center will need to provide purpose, dates, and times (estimated time
of arrival as well) they will need access to IOT Data Center Operations either calling 317-232-3245 or by email to notifyps1@iot.in.gov.

IOT Data Center Operations in-turn emails dcos@indiana.edu and DRTechnicalPlanning@iot.in.gov regarding the contractors and State employees visit email must include purpose, dates, and times. Any State employee or Contractor must sign in at the UITS Facilities Building and Data Center, 2737 East Tenth Street. Upon entering this facility; they will also be required to sign in at the operations desk before they will gain access to the machine room. They will be escorted by a university employee or a designated IOT state employee. At no time will a non-authorized state employee or state vendor without proper credentials be allowed access to the IU data center without an escort.

Roles
All Personnel

Responsibilities
Contractors, vendors, etc. shall abide by IOT Policy and Standards while on site at an IOT managed location. IOT shall follow badge access requirements for all employees and contractors. IOT shall promptly eliminate access to employees upon termination or loss of access card. Contractors will be provided with a temporary badge or contractor badge; badges should be returned on completion of project or deactivated if not returned. IOT employees requesting contractor access are responsible for explaining and ensuring adherence to this Standard. IOT employee is responsible to return temporary badges next business day after loan period expiration, extenuating circumstances should be communicated to badges issuer. Individuals not returning temporary badges will be charged the replacement fee of $20.00.

Management Commitment
Management is responsible for implementing and enforcing the Physical Access Security Standard within their supported area(s). Supervisors shall be responsible for ensuring that their employees comply with the requirements in this Standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary when access is required.

Compliance
The IOT Security Team shall review access and visitor logs for the IOT facilities every 180 days and investigate any unusual access. Further, IOT Security shall review access card rights for facilities every 180 days and remove access for individuals that no longer require access.

Exceptions
Exceptions will be handled on a case by case basis through the Director of Risk & Compliance and State CISO.