IOT PHYSICAL SECURITY

Practice 6.1.1

Issue Date: 05/21/2007
Effective Date: 05/21/2007

1. Purpose

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

2. Revision History

Revision Date	Revision Number	Change Made	Reviser
05/21/2007	01	Policy Draft	R. Baker
10/31/2007	02	Updated format to match with ISF V2.0 and standard policy documentation	C. Bradley
01/15/2008	03	Incorporated specific access procedures to IOT facilities	T. Stahl

3. Persons, Groups, Systems Affected

   IOT personnel, contractors and visitors

4. Policy

   IOT will secure and limit access to the datacenter, 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.

5. Responsibilities

   5.1. Contractors, vendors, etc –abide by IOT policy while on site at an IOT managed location.
   5.2. Indiana Office of Technology – to 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 return on completion or project or deactivated if not returned. IOT employees requesting contractor access are responsible for ensuring adherence to this practice.

6. Procedures

a. Badge Access practice 6.1.2 will be followed to ensure proper access for IOT personnel and contractors.
b. Managers are responsible for giving 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.
c. Managers and/or employees are responsible for promptly notifying appropriate personnel when access to IOT facilities has been terminated or suspended.
d. 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 should 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.
e. 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 50697

IOT Office Access

a. Normal Hours (7:00 a.m. – 4:30 p.m.)

IOT workforce (employees and contractors)

1. 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.
2. Managers shall request new or changed access for employees and contractors under their authority via the Help Desk system. Tickets are routed to the Security Section.
3. 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 a Help Desk Ticket unless there is an elevated security concern. In such cases, access control providers should be contacted directly.
4. Any employee losing an access card is to immediately contact Security via a Help Desk Ticket so that card privileges of the lost card can be eliminated.

Visitors (includes delivery and pickup)

1. Visitors without a State of Indiana security badge accessing IOT work areas are to be escorted.
2. Visitors should report to the front desk and await escort into the working area.
3. State employees (non-IOT) or contractors with a State of Indiana security badge may travel unescorted through IOT work areas.
4. IOT employees should not leave un-badged state employees or vendors in work areas without an escort.

Service personnel

Authorized service personnel (electricians, phone men, 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.

b. After Hours/Weekends/Holidays Access

IOT workforce (employees and contractors)

IOT staff is to have their access in terms of both time and location established by management and enabled on their parking pass/ID badge. Access to facilities,

outside of the originally prescribed window, must be requested by the responsible manager at least 24 hours prior to need for the changed access.

Visitors (includes delivery and pickup)

1. 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.
2. Visitors shall gain access through preplanned means and abide by all Government Center entry requirements.
3. 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 men, 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 should 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.

a. Normal Hours (7:00 a.m. – 4:30 p.m.)

IOT workforce (employees and contractors)

1. Requests for access to the North/South MDF, communication closets, and data center access are to be first approved by the Network Services Manager or the Data Center Manager.
2. Staff must follow the rules of conduct established by the owner for visitation and use of the facility.
3. 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 a Help Desk Ticket unless there is an elevated security concern. In such cases, access control providers should be contacted directly.

b. 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. Escort requirements and rules of conduct established by facilities owners are to always be obeyed.

7. Compliance

- IOT managers shall be responsible for implementing and enforcing the Physical Access Security Policy within their supported.
- Supervisors shall be responsible for ensuring that their employees comply with this policy.

- IOT Security shall be responsible for the review of access records and visitor logs for the IOT facilities on a periodic basis and investigate any unusual access.
- IOT Security shall be responsible for the review of the access card rights for the facilities on a periodic basis and remove access for individuals that no longer require access.
- All employees should question and report any unusual or unacceptable activities.