Tier 1 Control Standards (State-Wide)

IOT Badge Access

Standard ID
IOT-CS2-SEC-101

Published Date
1/15/2007

Effective Date
1/15/2007

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
This Standard defines how to gain a security badge from IOT. Physical access to the Indiana Office of Technology shall be restricted to only those workforce members needing access to perform their jobs. IOT employees and contractors are to have the minimum card access system rights required to complete their duties.

Scope
IOT

Statement
The following are the IOT Badge Access requirements:

- IOT managers shall determine the access required by staff and/or contractors to IOT facilities. Access rights should be the minimum necessary to execute job duties.
- Normal requests for access shall be requested via email to the Security Team. Emergency needs should be made known directly to the Security Team in person.
- Access to the data center and server team room shall be granted only with authorization from the Data Center Operation’s Manager or their designee.
- Access to the MDFs, communication closets and network lab shall be granted only with authorization from the Network Services Manager, Director of Infrastructure Services or their designee.
- Access to the KVM room shall be granted only with authorization from the Manager of Server Applications, Director of Infrastructure Services or their designee.
- Access to the deployment and dispatch room shall be granted only with authorization from the Desktop Refresh Manager, Director of Delivery Services or their designee.
- Access to Indiana Government South Tech room shall be granted only with authorization from the Director of Delivery Services.
- It is the responsibility of employees with lost or stolen access cards to immediately contact the Security Team. This can be accomplished by a phone call or through an email to the Security Team.
- Temporary access to facilities will be provided as authorized by an IOT manager. Access requirements and timeframes should be submitted to the Security Team via email. Managers are responsible for appropriately requesting the deactivation of the temporary access and returning the temporary access card to the Security team.
- Replacement of lost or stolen cards and associated costs of replacement are the responsibility of the employee, contractor or vendor to which the card was issued.
- Upon employee termination, managers should retain the former employee’s access/ID card, IU Access card ensure rights are
 enabled by the Security Team, and forward the card to their human resources contact.

- Managers with an employee changing roles should notify the Security Team with instructions to eliminate access required by previous duties.
- IOT abides by all IDOA policies regarding access cards.
- Access to UITS Facilities Building and Data Center, Bloomington shall be granted via email to the #IOT Disaster Recovery Technical Planning by the concerned management providing justification why the access is required along with the employee name and their state email address.
- The employee(s) have to collect their Access card and their Biometric Access onsite in accordance to IU Security compliance by showing proper identification.
- Employee/vendor termination has to be communicated #IOT Disaster Recovery Technical Planning by the concerned management so the team can email IU to revoke access.

Roles
IOT Personnel

Responsibilities
All IOT personnel are responsible for understanding the requirements written within this Standard.

Management Commitment
Management is responsible for determining the access required by staff and/or contractors in accordance with this Standard.

Coordination Among Organizational Entities
Managers shall coordinate with IOT Security and appropriate supervisors to obtain access in accordance with this Standard.

Compliance
The Security Team will audit access logs every 180 days or on request and notify managers of anomalies. The Security Team will audit terminated employees every 180 days ensuring their access has been eliminated. The Security Team will audit temporary cards on a quarterly basis.

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