P.14

Policy Name

Physical Security Policy

1. Purpose

The purpose of this Policy is to establish the requirements for physical security of all systems, personnel, and information/media where IOT has people or assets.

2. Scope

The Statewide IT Policies and Standards ("POLICIES") apply to all IOT-supported entities ("Entities"), their employees, their contractors, their consultants, and their vendors. Unless otherwise specified, all of the POLICIES apply equally to physical and electronic assets and resources assigned to an individual, on-premises physical assets, on-premises virtual assets, on-premises cloud assets, assets provided by cloud service providers, products and/or services that use cloud computing, all data stored or processed by the above assets in electronic, paper, or any other form, and everything else that supports the functioning of State government ("State Enterprise").

3. Policy

3.1 Definitions

a. "IOT Space" means:
   A space, other than a residence, where an IOT employee, contractor, or consultant works,
   A space IOT uses for storage, and
   A space where IOT hosts the processing of data.
b. "IOT Individual" means an IOT employee, contractor, or consultant.
c. "Visitor" means anyone other than an IOT Individual. Visitors include vendors and employees of other state agencies.

3.2 Statement Regarding IOT Individuals

a. IOT must establish some control of public access to IOT Space.
b. IOT must provide an IOT Badge for authorized IOT Individuals.
c. An IOT Individual must wear his or her IOT Badge and keep it visible at all times while in IOT Space.
d. IOT managers are responsible for maintaining the accuracy of an IOT Individual's badge configuration by updating IOT Security regarding necessary changes.
e. IOT Security may manage the configuration of IOT Individuals' badge access. IOT Security needs at least 24 hours' notice to prepare appropriate badge configuration for an IOT Individual, regardless of whether it is the initial
a. configuration of badge access for that IOT Individual, a revision of that IOT Individual's badge access, or a termination of that IOT Individual's badge access.
f. IOT Security may issue a Temporary IOT Badge for no more than thirty calendar days.
g. In configuring an IOT Individual's access to physical areas, IOT will provide physical access to only those areas required for performance of the IOT Individual's duties.
h. An IOT Individual must notify IOT Security within an hour of discovering that his or her badge has been lost or stolen.
i. Tailgating is prohibited. An IOT Individual must present or scan his or her badge, as appropriate, regardless of whether a door or other means of ingress/egress is open.
j. IOT Individuals should report suspicious behavior to their manager. Managers are responsible for escalating any suspicious behavior.
k. IOT may use surveillance in IOT Space. There is no expectation of privacy in IOT Space.
l. IOT managers will review monthly: logs of physical access to IOT Space for purposes of identifying noncompliance with this Policy.
m. To the degree that an IOT Individual works out of another Entity's location, he or she must review, understand and comply with the respective Entity's policies and procedures.

n. An IOT Individual must lock a computer or mobile device when leaving it unattended in IOT Space.
o. On the last day of an IOT Individual's service to IOT, the IOT Individual's manager must meet with the IOT Individual to receive all physical tools assigned to the IOT Individual, including the IOT Badge, workstation, cell phone, tablet, headphones, and anything else they have been assigned. Also, the IOT Individual's manager must notify IOT's Identity and Access Management team to terminate the IOT Individual's physical and electronic access. The IOT Individual's manager must confirm that the IOT Individual's physical and electronic access was terminated.

3.3 Statement Regarding Visitors

a. IOT may provide a Visitor Badge for a Visitor upon sign-in.
b. A Visitor must wear and keep the Visitor Badge visible at all times. A Visitor must return the Visitor Badge when leaving the IOT Space. IOT will maintain a log of its providing and retrieving of Visitor Badges.
c. The Visitor Badge must be visibly different from the IOT Badge.
d. A Visitor may not enter or remain in an IOT Space without the presence of an IOT Individual. If a Visitor is observed to be without escort, an IOT Individual should escort the Visitor. Visitors must be escorted at all times.
e. IOT will not allow deliveries or service outside the normal business hours of the respective building unless an IOT manager has made a written confirmation of the delivery.
f. IOT may communicate other rules for Visitors.
g. This Policy does not apply to environmental services personnel.

3.4 Spaces of Increased Protection

a. IOT may adopt more stringent provisions regarding the physical security of data centers, disaster recovery sites, main distribution frames, intermediate distribution frames, and other physical areas of increased sensitivity.

4. Exceptions

Exception Requests will be addressed through the process designated by IOT.

5. Ultimate Authority

The Chief Information Officer is the ultimate authority for decisions made pursuant to the POLICIES, including Exception Requests.

6. Roles and Responsibilities

State agencies vary tremendously. Some State agencies have Chief Information Officers, while others may have no dedicated IT employees. Because of that variance, the Statewide IT Policies and Standards do not refer to a specific job title as being responsible for compliance. Instead, the intent is for the responsibilities to rest with the agency head or the highest-ranking employee responsible for IT, unless stated otherwise regarding a specific duty.

7. Statutory Purposes

The statutory purposes of IOT include "establish the standards for the technology infrastructure of the state" and "provide for the technology and procedures for the state to do business with the greatest security possible," Ind. Code § 4-13.1-2-1(1) and (5). IOT has an obligation to "develop and maintain policies, procedures, and guidelines for the effective and secure use of information technology in state government," Ind. Code § 4-13.1-2-2(a)(11).

8. Industry Standards

The Statewide IT Policies and Standards are based on the following:

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, U.S. National Institute of Standards and Technology, Special Publication 800-37 Rev. 2. https://csrc.nist.gov/pubs/sp/800/37/r2/final

Security and Privacy Controls for Information Systems and Organizations, U.S. National Institute of Standards and Technology, Special Publication 800-53 Rev. 5. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Critical Security Controls v.8.1, Center for Internet Security. https://www.cisecurity.org/controls

9. Federal Audit

The federal government audits the IT practices of several Entities. Where necessary, those Entities may create agency-specific policies to supplement the Statewide IT Policies and Standards. Those agencies include the Bureau of Motor Vehicles, Department of Child Services, Department of Revenue, Department of Workforce Development, Family and Social Services Administration, Indiana Office of Technology, and the Indiana State Police.