P.07

Policy Name

Encryption and Cryptography Policy

1. Purpose

This Policy establishes the requirements for protecting IOT, agency, and citizen data while in transmission or at rest, both internally and externally. Sensitive data should be protected with administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability.

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 Encryption of Data in Transit

a. Sensitive information must be encrypted during transmission.
b. Transmission of data must be encrypted based on sensitivity level and State or Federal guidelines for secure data transmission. Please refer to the Data Classification Policy and Standard for further guidance.
c. All wireless connections must be encrypted. Please refer to the Encryption and Cryptography Standard for further guidance.
d. To connect to the network, an individual must be on an approved or sponsored device. Where permitted, individuals connecting to the network with a nonstate-provided device must connect through an encrypted connection.
e. Connections between IOT, Entities, and other providers, such as public cloud vendors, must be encrypted.

3.2 Encryption of Data at Rest

a. Data at rest must be encrypted. The Data Classification Standard outlines requirements for encryption based on sensitivity level.
b. Full disk encryption should be used when it is technically feasible and is the preferred method for encrypting software on databases and all data center infrastructure (e.g., servers, storage, and network).
c. IOT must provide disk encryption on all end-user devices.
d. All data stored or managed in cloud environments must be encrypted while at rest by the application managing the cloud environment. Regular reviews must be conducted to make sure that cloud environments follow all IOT encryption policies and standards.
e. Removable media are rarely permitted. All removable devices must be encrypted and use approved encryption algorithms outlined in the Encryption and Cryptography Standard.

3.3 Key Generation and Encryption Management

a. For all encryption referenced in this Policy, IOT and Entities must use secure, nondeprecated encryption algorithms. Please refer to the Encryption Standard for further guidance.
b. For all encryption referenced in this Policy, IOT and Entities must use only industry-standard encryption keys and industry-standard means of generating keys.
c. IOT must maintain physical and logical access control to key-generating tools and procedures. IOT must use least privilege in determining who may access the key-generating tools and procedures.

d. A documented key-rotation procedure and schedule must be implemented, including an annual rotation of master keys.
e. The use of any encryption or encryption tool other than that provided by IOT is prohibited.
f. Keys used for encrypting data at rest must be backed up following a documented and proven recovery process.

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.