P.08

Policy Name

Enterprise Resiliency Policy

1. Purpose

This Policy establishes requirements for maintaining the continuity of operations and establishing resilient business processes. This Policy also establishes a framework for ensuring proper emergency response and disaster recovery.

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 Business Continuity and Disaster Recovery Planning

a. IOT and Entities must have a documented Business Continuity Plan ("BCP") and an IT Disaster Recovery Plan ("DRP").
b. The BCP and DRP must be stored in multiple secure locations, ensuring their availability and resilience during disruptive events. At least one location must be non-digital.
c. Copies of the BCP and DRP must be distributed to key contingency personnel.
d. Plans must be updated and distributed to IOT and the Indiana Department of Homeland Security at defined intervals and in accordance with State requirements.
e. The BCP and DRP must be stored on-premises, off-premises, and in separate physical locations.

3.2 Developing and Implementing BCPs and DRPs

a. The BCP and DRP must address the required capacity to support critical missions and business functions, define recovery objectives and priorities, and identify roles and responsibilities.
b. Alternative storage and processing sites must be identified (permanent and/or temporary) at least 25 miles from the primary facility and configured with security measures equivalent to the primary site. IOT and Entities must establish the necessary third-party service agreements to allow for the resumption of information systems for operations of critical business functions within the time defined in the BCP or DRP (e.g., priority of service provisions).
c. Emergency power, backup telecommunications, and backup internet service must be available at the main site.
d. Alternate telecommunications and internet services must be established and sufficiently separated from the primary service provider.
e. The recovery and reconstitution of the information system, after a failure or other contingency, must be completed in a trusted, secure, and verifiable manner so that recovery can be validated.
f. IOT and Entities must identify critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to operations, staffing, materials, transport, facilities, and other aspects.
g. Business impact analyses should be used to evaluate the consequences of disasters, security failures, loss of service, and service availability.

3.3 Resiliency

a. Resiliency requirements to support the delivery of critical services must be established for all operating states (e.g., under duress/attack, during recovery, normal operations).

b. IOT and Entities must identify their place in critical infrastructure, specifically noting interconnections and integrations with other agencies, governments, and private organizations, where applicable.
c. Dependencies on critical functions must be established and considered when developing the BCP and DRP, including both internal and third-party-hosted systems.
d. Resiliency practices must be considered in the build and design of all information systems.
e. Information security requirements and considerations must be included and considered in all forms of resiliency planning.

3.4 Back-Up and Disaster Recovery

a. IOT must establish and maintain disaster recovery practices sufficient to restore enterprise assets to a pre-incident and trusted state.
b. IOT and Entities must perform backups weekly or more frequently, based on the sensitivity of the data.
c. Automated tools should be used to track the success of all backups.
d. The integrity and security of the backup copies must be maintained to ensure future availability. IOT should establish and maintain an isolated instance of all recovery data. Any potential accessibility problems with the backup copies must be identified and mitigated in the event of an area-wide disaster.
e. All data backups must be encrypted. In addition, backups must align to the retention, disposal, and destruction process. This includes establishing data protection control equivalency to the original data.
f. Backup and recovery processes and associated timelines should be reviewed at least annually to validate that defined recovery metrics and methods continue to meet business objectives.
g. Data backup and recovery processes must be tested on a periodic basis, at least twice per year, for a sampling of enterprise assets.

3.5 Communications

a. A disaster exists when so declared by an authorized person.
b. Recovery communication plans must be established and tested during business continuity and disaster recovery testing scenarios.
c. Recovery communications must include defined and scheduled communication mechanisms and relevant stakeholders. Preapproved and standardized communication templates should be created and used.
d. Public relations must be included in the BCP and DRP and include considerations for reputational repair and messaging to the public.

3.6 Testing, Maintaining, and Re-Assessing Business Continuity Plans

a. IOT and Entities should use a variety of testing techniques (e.g., tabletop exercises, live simulations) to provide assurance that the BCP will operate during an actual event.
b. The BCP and DRP should incorporate lessons learned from actual events and live scenarios.
c. The BCP and DRP should be reviewed annually and updated when changes to the environment warrant.

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.