Tier 1 Control Standards (State-Wide)

Business Continuity

Standard ID
IOT-CS-SEC-015

Published Date
10/10/2017

Effective Date
11/1/2017

Last Updated
1/19/2018

Next Review Date
1/19/2019

Policy
20.0 Recovery Planning (RC.RP)
20.1 RC.RP-1

20.1.1 Recovery Plan Execution

Purpose
Define the requirements to establish and update a Business Continuity Plan and provide distinction between Continuity of Operation Plan (COOP) and Disaster Recovery Plans

Scope
IOT Supported Entities

Statement
Business Continuity (BC) plans are developed to maintain or restore business operations in the required time frames following interruption to, or failure of, information resources that support critical business processes. Each agency business continuity plan must be focused on restoring specific services to customers, both internal and external, in acceptable amount of time. The services and resources that are needed for this recovery process to occur must be carefully considered, including technical fail-over equipment, staffing requirements, backup requirements, Recovery Time and Recovery Point objectives (RTO and RPO), etc.

Agencies must develop a Business Continuity Plan and update the document on an annual basis. At minimum, the plan must contain the following:

- Method of invoking the plan and who is authorized to invoke the plan
- Identification and agreement of all responsibilities and emergency procedures
- Contact information including emergency contact information for participants
- Resources (personnel, facilities/premises, technologies and communications, information, supplies) required for restoration of business services
- Business Impact Analysis
  - Schedule of principle tasks to be completed and responsibilities for each task
  - A list of services to be recovered in prioritized order
  - Implementation of procedures that allow recovery and restoration of business services in the required time frames
  - Detailed documentation of procedures and processes
  - Applications and data criticality analysis
- A Disaster Recovery Plan (for all critical systems)
Business Impact Analysis (BIA)

To fulfill the requirements of the Business Continuity Plan, a Business Impact Analysis must be completed and reviewed periodically. Identification of events that can cause interruptions to business processes (e.g., equipment failure, vendor failure, flood or fire) and the resulting impact of interruptions must be considered when performing the analysis. The Business Impact Analysis should take into consideration threats that may disrupt the business operations such as:

- Malicious activity (criminal or deliberate actions)
- Natural disasters (flood, earthquake, tornado, blizzard)
- Technical issues (loss of service, hardware failure, software failures)
- Human resources issues (pandemic, labor disputes/strikes)
- Geographic factors
- Geo-political factors

The analysis shall evaluate the potential effects of such events and the cascading impacts that could result.

Disaster Recovery

Disaster Recovery Planning (DRP) is a component of an agency’s Business Continuity Plan (COOP – Continuity of Operation Plan) which is handled by the Indiana Department of Homeland Security (IDHS). Please refer to standard 20.1.1 Disaster Recovery for more information.

Agencies are responsible for prioritizing critical systems in their COOP and working with IOT on a plan for recovering their systems in the secondary data center in case the primary data center is impacted in a disaster event.

A Disaster Recovery Plan should not be intermingled as a High Availability solution or option offered by IOT. The Service Level Agreement dictates day to day operations and business continuity while Disaster Recovery concentrates on the IT recovery of critical systems hosted in the IOT Data Center, provided the agency has partnered with IOT to have a Disaster Recovery Plan.

Agencies shall refer to IOT Service Level Agreements to understand the recoverability of systems during outages. Further, agencies shall collaborate with IOT to manage High Availability (HA) capabilities as part of their Business Continuity Plan.

Roles

Agency Management
Agency Personnel
Information Asset Owners/System Owners

Responsibilities

Agency Security/System Owner will develop the Business Continuity, Business Impact Analysis, and Disaster Recovery Plans in accordance with the requirements written within this Standard.

Management Commitment

Agency Management is responsible for ensuring their agency has an up to date Business Continuity Plan that meets the requirements of this Standard and the agency needs.

Coordination Among Organizational Entities

Agencies shall coordinate with DHS and IOT where necessary to document their plan as it pertains to this Standard.

Compliance

Agencies that do not document a Business Continuity Plan in accordance with the Governor's Executive Order 13-09, "Continuing the Governor's Emergency Advisory Group", and Executive Order 17-02, "Continuing the Governor's Emergency Advisory Group and other Emergency Measures" may be subject to enforcement by DHS.

Exceptions

Exceptions will be handled on a case by case basis by the CIO or CISO.
Associated Links
Executive Order 13-09
Executive Order 17-02

Attachments
BIA Standards.docx
Multi-Site HA-Same Site HA-DR Failure and support matrix.pdf
IOT Teams Policy for COOP-BC.docx