Office of Information Technology
Policy

Disaster Recovery / Business Continuity Planning Policy

Policy:
Agencies must develop, test and maintain disaster recovery/business continuity plans designed to ensure the availability of mission-critical services and functions in the event of a disaster or unscheduled event that impacts the agency's information technology or telecommunications systems. Agencies shall utilize the current DR/BC planning software hosted by OIT.

Scope:
This policy is applicable to all entities under the authority of the Office of Information Technology, pursuant to the provisions of R.S. 39:15.1, et seq., which provide mission-critical services to the public, local government, federal government and other state agencies.

Responsibilities:
Agencies are required to develop and regularly update disaster recovery/ business continuity plans using the guidelines noted below. Additionally, an electronic copy of the most recent DR/BCP must be submitted to the OIT Security Office annually.

- Business Impact Analysis - Conduct risk assessment and document the potential impacts of likely event to the agency. With each risk, an analysis of the likelihood of event should be determined and prioritized in such a manner so that methods of mitigation can be explored. Understand the effect that a business interruption will have on the agency's ability to deliver services. Long and short term interruptions should be considered in this analysis. A worst case event should be assumed and agency business process alternate procedures established, recovery time objectives determined, and recovery priority organized by criticality.
- Develop an agency Disaster Recovery/ Business Continuity Plan (DR/BCP) – Develop a DR/BCP based on accepted industry best practices. The plan should be created to support the agency's business objectives and priorities. The plan must be entered and maintained within the DOA hosted instance of LDRPS according to the OIT LDRPS Compliance Guidelines.
- Testing and Updating the Plan - Plans must be tested to verify they are effective. Regular updates to the plans are necessary to keep information and processes accurate.
- Management of the Plan - Agency leadership sponsors and supports the plan. Responsibilities for the plan will be distributed across the agency organization and require support from all levels of management

Owner:
OIT Security Office

Related Policies, Standards, Guidelines:

Office of Information Technology
Policy

OIT LDRPS (Living Disaster Recovery Planning System) Compliance Guidelines

Effective Date:
July 27, 2009