Operational Policy

Policy title:	**Disaster Recovery Policy for Information Technology**		
Policy number:	DHS|OHA 070-006		
Original date:	07/06/2020	**Last update:**	07/06/2020
Approved:	Don Erickson, DHS Chief Administrative Officer Kris Kautz, OHA Deputy Director		

Purpose

The Department of Human Services (DHS) and the Oregon Health Authority (OHA) are committed to establishing a disaster recovery policy for information technology (IT) that supports and meets the agencies' goal of service excellence through the appropriate protection, review, and recovery of data.

Description

Information systems are essential to an organization's success. It is critical that identified services provided by these systems can operate effectively without excessive interruption. This policy requires DHS|OHA to plan for and respond to disasters that may cause disconnections from or outages of the agencies' IT systems.

Applicability

This policy applies to all DHS and OHA staff including employees, volunteers, trainees, interns, as well as contractors and partners.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rule, and state and federal law. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Policy

1. Disaster recovery (DR) means restarting technology operations after an outage using policies and processes prepared for recovery or continuation of mission-essential technology infrastructure after a disaster. These processes are found in a DR Plan. The principle goal of DR plan is to resume critical processes.
2. Each DHS|OHA application shall have a DR plan created using the approved DR plan template.
   a. DHS|OHA applications that are Cloud native are not required to complete a DR plan template but are required to verify DR resiliency.
      A. Cloud native is an application that is specifically designed to utilize services and infrastructure from cloud service providers.

B. Resiliency is the ability to quickly adapt to and recover from any known or unknown changes to the environment.

b. Any mission critical application unable to comply with this policy shall have a risk assessment completed and an exception approved by the Office of Information Services (OIS) Chief Information Officer (CIO), with plans to remediate identified gaps.

3. DR plans shall be stored in a centralized location, electronic and hard copy.
4. Each application owner shall review and update their DR plan whenever a major application change occurs such as role change or application configuration.
5. The following maintenance activities shall be conducted annually for mission critical applications:
   a. Update the documented DR plan.
   b. Review the DR objectives and strategies.
   c. Update the internal and external contacts list.
   d. Perform a functional exercise to validate the DR plan. A functional exercise is an exercise that allows personnel with operational responsibilities to validate their IT plans and their operational readiness for emergencies in a simulated operational environment.
6. The following maintenance activities shall be conducted annually for business critical and business important applications:
   a. Update the documented DR plan.
   b. Review the DR objectives and strategies.
   c. Update the internal and external contacts list.
   d. Conduct a tabletop exercise to validate the DR plan. A tabletop exercise is a discussion-based exercise where staff with roles and responsibilities in the DR plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles and their responses to a particular emergency situation.

References

Use IT Disaster Recovery Tiering to Build a Recovery Strategy That Works, Gartner
DAS 107-001-010 Statewide Continuity of Operations Planning Policy
DHS|OHA 070-006-01 Disaster Recovery Process for Information Technology
DHS|OHA 070-006-02 Disaster Recovery Process for Information Technology Process Map
DHS|OHA 100-06 Business Continuity Planning Policy
Microsoft Cloud Native Applications
A Microsoft Word Document Template for Disaster Recovery Planning
National Institute of Standards and Technology (NIST) Special Publication 800-34 Rev. 1
NIST SP 800-84
Sdxcentral: What is Cloud Native?

Application Criticality

Tier	Criticality	Business Process	Recovery Point Objective (RPO)	Recovery Time Objective (RTO)
Tier 0	Foundational IT core services	Critical IT infrastructure such as network services, domain name services (DNS), directory services, access controls	Must be operational prior to mission critical services	Must be recovered with or prior to mission critical RTOs for business services
Tier 1	Mission critical	Critical business function that is life, safety, financial impacting Generally public facing	Zero hours to 1 hour	Zero hours to 1 hour
Tier 2	Business critical	Internal operations and/or customer focused	One to four hours	One to four hours
Tier 3	Business important	Internal, with alternative operations models	Four to twenty-four hours	Four hours to forty-eight hours

Definitions

1.Recovery Point Objective (RPO) is the maximum acceptable amount of data loss measured in units of time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs. RPO referenced in this policy reflects current industry standard.

2. Recovery Time Objective (RTO) is the duration of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable. RTO referenced in this policy reflects current industry standard.

Forms referenced
Disaster Recovery Plan Template

Contact
Office of Information Services
Service Desk: 503-945-5623
ois.servicedesk@dhsoha.state.or.us

Policy history
Version 1 Established joint DHS|OHA 070-006 policy xx/xx/xxxx

Keywords
Application recover test, applications, business critical, business important, Cloud native, disaster, disaster recovery, drill, mission critical, recovery, Recovery Point Objective, RPO, Recovery Time Objective, RTO, resiliency, Tier 1, Tier 2, Tier 3
