Process steps

Title:	DHS|OHA 070-006-01 Disaster Recovery Process for Information Technology
Related to:	DHS|OHA 070-006 Disaster Recover Policy for Information Technology
Effective date:	07/06/2020

Purpose

This process outlines the necessary steps for the execution of a disaster recovery plan for applications managed or owned by the Office of Information Services (OIS). The Department of Human Services (DHS) and the Oregon Health Authority (OHA) are committed to establishing a disaster recovery process for information technology (IT) that supports and meets the agencies' goal of service excellence through the appropriate protection, review, and recovery of data.

Applicability

This process 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.

Process Steps

1. Staff from the Office of Information Services and program staff responsible for each DHS|OHA application create a disaster recovery (DR) plan in accordance with DHS|OHA 070-006. DHS|OHA applications that are Cloud native 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.
2. Responsible staff review and update DR plans annually, including verifying internal and external contacts lists. DR plans and contact lists are stored in a centralized location, in electronic and hard copy.
3. The recovery location and resources are identified in the application DR plan.
4. Maintenance activities are conducted annually for mission critical, business critical, and business important applications. (Refer to DHS|OHA 070-006)
   a. Functional exercises are performed annually for mission critical applications to validate the DR plan.

b. Tabletop exercises are conducted annually for business critical and business important applications to validate the DR plan.

5. When a significant outage or disruption event affects DHS|OHA applications, a disaster recovery plan for the application is executed.
   a. See examples of possible outage or disruption events in the references.
   b. The outage event may result in damage to the facility that houses the application, damage or loss of equipment, or other damage that typically results in long-term loss.
6. The response phase outlines the immediate actions following a significant event.
   a. Staff authorized to activate a disaster recovery plan (see references) contact the responsible parties identified in the application's disaster recovery plan.
   b. The responsible parties:
      A. Communicate the outage event or issue to applicable stakeholders.
      B. Prioritize what actions need to be taken first.
      C. Identify additional resources needed for recovery.
      D. Establish a primary and secondary conference line for a bridge to coordinate next steps as outlined in the DR plan. Communicate the specific recovery roles and determine which strategy will be pursued.
      E. Create a disaster recovery event command center, as needed.
7. The recovery phase includes activities necessary to resume services after the outage event. Designated staff are identified to complete the recovery steps. The recovery of every application will be slightly different depending on its' construction and type of disaster event.
8. Designated staff:
   a. Verify availability and functionality of recovery locations.
   b. Verify the availability and functionality of required resources to recover the application.
   c. Retrieve required resources.
   d. Recover hardware and operating system as needed.
   e. Recover application from back-up.
   f. Configure application.
   g. Restore data from back-up.
9. During the restoration phase designated staff outline tasks to restore service to previous levels; the recovered application is rebuilt to operational status. Staff designated to complete the recovery steps are also responsible for the restoration phase.
10. Designated staff:
    a. Complete validation data testing. Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely.
    b. Complete validation functionality testing. Validating functionality testing is the process of verifying that the application functionality has been tested, and the system is ready to return to normal operations.
    c. Complete interface testing to validate that the communication between systems is functional and the application is ready to return to normal operations.
    d. Notify relevant parties outlined in the disaster recovery plan that full restoration of the application and services to pre-event levels has occurred and that the recovery effort is complete.

References

DHS|OHA Staff Who May Activate DR Plan for Application
1. Chief Information Officer (CIO)
2. Deputy Chief Information Officer (DCIO)
3. OIS IT Director
4. OIS Service Desk Manager
5. DHS|OHA Business Continuity Plan Coordinator
6. DHS|OHA Workplace Incident Response Coordinator
7. DHS|OHA Emergency Preparedness Coordinator

Dependencies

This section outlines the dependencies made during the development of disaster recovery plans. If and when needed the parties responsible for disaster recovery for the application will coordinate with their partners and contractors as needed to enable recovery.

Dependency	Assumptions
User Interface/Rendering Presentation components	• Users (end users, power users, administrators) are unable to access the system through any part of the instance (e.g. client or server side, web interface or downloaded application). • Infrastructure and back-end services are still assumed to be active/running.
Business Intelligence/Reporting Processing components	• The collection, logging, filtering, and delivery of reported information to end users is not functioning (with or without the user interface layer also being impacted). • Standard backup processes (e.g. tape backups) are not impacted, but the active/ passive or mirrored processes are not functioning. • Specific types of disruptions could include components that process, match and transforms information from the other layers. This includes business transaction processing, report processing and data parsing.
Network Layers Infrastructure components	• Connectivity to network resources is compromised and/or significant latency issues in the network exist that result in lowered performance in other layers. • Assumption is that terminal connections, serially attached devices and inputs are still functional.
Storage Layer Infrastructure components	• Loss of SAN, local area storage, or other storage component.
Database Layer Database storage components	• Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable.
Hardware/Host Layer Hardware components	• Physical components are unavailable or affected by a given event.
Virtualizations (VM's) Virtual Layer	• Virtual components are unavailable. • Hardware and hosting services are accessible.

Administration **Infrastructure Layer**	• Support functions are disabled such as management services, backup services, and log transfer functions. • Other services are presumed functional.
Internal/External Dependencies	• Interfaces and intersystem communications corrupt or compromised.

References Continued

Use IT Disaster Recovery Tiering to Build a Recovery Strategy That Works, Gartner
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?
OIS Incident Process Quick Reference Guide
OIS Incident and Change Process Integration for Major Incidents
DHS|OHA 070-006-02 Disaster Recovery Process for Information Technology Process Map

Related policies

DAS 107-001-010 Statewide Continuity of Operations Planning Policy
DHS|OHA 070-006 Disaster Recovery Policy for Information Technology
DHS|OHA 100-006 Business Continuity Planning Policy

Forms referenced

Disaster Recovery Plan Template

Contact

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

Process history

Version 1 Established joint DHS|OHA 070-006-01 process 07/06/2020

Keywords

Application, assumptions, back-up, dependency, disaster, disaster recovery, disaster recovery plan, event, interface, recovery phase, response phase, significant outage, validation data testing, validation functionality testing

---