Omeka Services IT Contingency Plan

INTRODUCTION

The Corporation for Digital Scholarship operates without a centralized physical location. As a result, most elements of disaster recovery planning are mitigated by the distributed locations of the leadership and staff. CDS maintains a virtual office in Vienna, Virginia, but the corporation officers are located all over the world. As a result, the primary requirements for continuous operations are internet and wireless access. It is difficult to imagine a scenario where an event, short of a catastrophic global disaster, would disrupt those elements for all of the officers, and in such a case the continuity of operations for CDS would likely be low on anyone's priority list.

Nonetheless, more minor an immediate events might work to disrupt service to one or more of the products and services that CDS offers to the public. This Omeka Services Contingency Plan establishes procedures to recover Omeka Services web hosting following a disruption. The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    a. Notification/Activation phase to detect and assess the damage and to activate the plan
    b. Recovery phase to restore temporary IT operations and recover damage done to the original system
    c. Reconstitution phase to restore IT system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out Omeka Services processing requirements during prolonged interruptions to normal operations.

3. Assign responsibilities to designated Omeka personnel and provide guidance for recovering Omeka Services during prolonged periods of interruption to normal operations.
4. Ensure coordination with other CDS staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

APPLICABILITY

The Omeka Services Contingency Plan applies to the functions, operations, and resources necessary to restore and resume Corporation for Digital Scholarship's Omeka Services operations as it is installed at Amazon Web Services. The Omeka Services Contingency Plan applies to CDS and all other persons associated with Omeka Services as identified under Section 2.3, Responsibilities.

SCOPE

Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on three key principles.

1. The Corporation for Digital Scholarship's resources hosted at Amazon Web Services are inaccessible; therefore, Corporation for Digital Scholarship is unable to perform Omeka Services processing for subscribers.
2. The Corporation for Digital Scholarship's resources hosted at Amazon Web Services with multi-site location redundancy.
3. The software applications required to establish and run Omeka Services are available via the Corporation for Digital Scholarship's Omeka project Github repositories and local hardware distributed through the Omeka Services team.

Assumptions

Based on these principles, the following assumptions were used when developing the IT Contingency Plan:

1. The Omeka Services is inoperable at the Corporation for Digital Scholarship's Amazon Web Services hosting and cannot be recovered within 12 hours.
2. Key Omeka Services personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the Omeka Services Contingency Plan.
3. Current backups of the application software and data are intact and available via Amazon Web Services and Github.

4. Service agreements are maintained with Omeka Services hosting providers to support the emergency system recovery.

This plan should be reviewed annually and updated as necessary.

CONCEPT OF OPERATIONS

SYSTEM DESCRIPTION AND ARCHITECTURE

1. Omeka Services uses Amazon EBS as its data storage: https://aws.amazon.com/ebs/features/#Amazon_EBS_Elastic_Volumes
2. The files are stored in S3 which has very high guarantees for the data stored in it: https://docs.aws.amazon.com/AmazonS3/latest/dev/DataDurability.html
3. The databases are backed up daily with a process running on the server. The backups are stored on the same EBS volume as are the rest of the server instances.
4. The system is set up to also take daily snapshots that we maintain for a week, in the very unlikely case of a drive failure.

LINE OF SUCCESSION

The Corporation for Digital Scholarship sets forth an order of succession to ensure that decision-making authority for the Omeka Services Contingency Plan is uninterrupted. The Director of the Omeka project is responsible for ensuring the safety of personnel and the execution of procedures documented within this Omeka Services Contingency Plan. If the Director is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the President of CDS shall function as that authority.

1. Sharon Leon, Director of Omeka and Vice President of CDS [Location: East Lansing, MI]
    a. Sean Takats, President of CDS [Location: Paris, France]
2. John Flatness, Omeka Lead Developer [Location: Fairfax, VA]
    a. Ken Albers, Omeka.net Manager [Location: Fairfax, VA]
    b. Jim Safely, Senior Omeka Developer [Location: Fairfax, VA]

RESPONSIBILITIES

The following staff have trained to respond to a contingency event affecting the IT system. The Contingency Plan establishes several teams assigned to participate in recovering Omeka Services operations.

Management/Coordination

Group to assure that all assessment, recovery, testing, and client communications work flows smoothly and that the entire staff is well informed of Omeka Services' status.

- Point Person: Sharon Leon

    - Sean Takats
- John Flatness

Damage Assessment

Group to investigate the cause and extent of the disruption, and determine whether a larger systematic response is necessary.

- Point Person: John Flatness
- Ken Albers
    - Jim Safely

System Recovery

Group tasked with doing the technical recovery work that might be necessary to bring back up servers, restore databases, and redeploy applications in the face of a disruptive event.

- Point Person: John Flatness
- Jim Safely
- Ken Albers

Testing

Group tasked with testing the functioning and completeness of Omeka Services after recovery work.

- Point Person: Ken Albers
- Megan Brett
- Sharon Leon

Communications

Group tasked with communicating with users and clients about disruptive events and the steps taken to mitigate and recover from them.

- Point Person: Ken Albers
- Sharon Leon
- Megan Brett

NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Omeka Services. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator.

In an emergency, the Corporation for Digital Scholarship’s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Notification Procedures

Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

1. The first responder is to notify the Contingency Planning Coordinator. All known information must be relayed to the Contingency Planning Coordinator.
2. The Coordinator is to contact the Damage Assessment Lead and inform them of the event, and ask them to begin assessment procedures.
3. The Damage Assessment Lead is to notify team members and complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time.

Damage Assessment Procedures

(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.)

1. Upon notification from the Contingency Planning Coordinator, the Damage Assessment Group Leader is to perform an initial assessment of the situation. Then, the Damage Assessment Group is to determine the extent of the damage to the servers, application software, and data, to determine the cause, and to create a plan to mitigate any further damage or loss, prevent the problem from reoccurring, and restore the Services.
2. When the damage assessment has been completed, the Damage Assessment Group Leader is to notify the Contingency Planning Coordinator of the results.
3. The Contingency Planning Coordinator is to evaluate the results and determine whether the contingency plan is to be activated. The Contingency Plan is to be activated if one or more of the following criteria are met:
    a. Omeka Services will be unavailable for more than 4 hours because of a server disruption at AWS
    b. Omeka Services will be unavailable for more than 4 hours because of a hacking event.
4. If the plan is to be activated, the Contingency Planning Coordinator is to notify the System Recovery Group and inform them of the details of the event.
5. The Contingency Planning Coordinator is to notify remaining Omeka Dev Team (via notification procedures) on the general status of the incident.

RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

Recovery Goal: To return internet access to Omeka Services installations so that clients and users have full web access to the public and administrative interfaces for their work.

1. Communications Group
    a. Inform clients of disruption and estimated time to restoration of service
    b. Update clients every 12 hours if disruption continues longer than estimated

2. System Recovery Group
    a. Server failure scenario:
        i. Establish maintenance mode
        ii. Shut down existing servers
        iii. Establish fresh servers
        iv. If database is not corrupted, run a dif between current database and the most recent back-up to assess content loss between freeze and backup
        v. Redeploy core software application from Github
        vi. Reinstall add-ons from github
        vii. Restore content from most recent database back-up
        viii. Restore customized theme from backup
        ix. Notify testing team
    b. Cyber attack/Hacking scenario:
        i. Establish maintenance mode
        ii. Isolate the point of intrusion and identify the areas of destruction
        iii. If database is not corrupted, run a dif between current database and the most recent back-up to assess content loss between freeze and backup
        iv. Patch or repair the corrupted code if possible
        v. If repair is not possible, redeploy core software application from Github
        vi. Reinstall add-ons from github
        vii. Restore content from most recent database back-up
        viii. Restore customized theme from backup
        ix. Notify testing team

3. Testing Group
    a. Review the functionality of the core Omeka installation and plugins from the administrative perspective.
    b. Review the sites from the end-user perspective, across browsers and operating systems.
    c. Alert the System Recovery Group to issues for remediation as necessary.

d. Retest as necessary.
e. Once testing is satisfactorily complete, notify the System Recovery Team and the Communications group

RETURN TO NORMAL OPERATIONS

1. System Recovery Group
    a. Remove Omeka Services from maintenance mode
    b. Restore full access to the client sites at the original domain name.
    c. Monitor access and performance for 48 hours

2. Communications Group
    a. Notify clients that service has returned to normal operations and will continue under close observation for the next 48 hours.

PLAN APPENDICES

Appendix A: Personnel Contact List
Appendix B: Vendor Contact List
Appendix C: Equipment and Specifications

RECORD OF CHANGES:
Reviewed and updated May 15, 2019 -- SML