Disaster Recovery Plan

The Reveal Disaster Recovery Plan ("DRP") establishes procedures to recover Reveal operations following a disruption resulting from a disaster. The types of disasters contemplated by this plan include natural disasters, political disturbances, man made disasters, external human threats, and internal malicious activities. This DRP is maintained by the CTO.

Disaster Recovery Policies

- Reveal performs testing of the Disaster Recovery Plan annually. The CTO is responsible for coordinating and conducting rehearsals of this Disaster Recovery Plan annually.
- Whenever the DRP is used, it must be followed by a retrospective and tabletop reenactment in order to identify lessons learned and playbooks needing creation.
- This policy and plan must be updated at least annually with additional playbooks taking into account new risks of disasters learned through testing and reenactment of past disaster incidents.

Scope of Disaster Recovery Plan

This policy includes all resources and processes necessary for service and data recovery, and covers all information security aspects of business continuity management.

The following conditions must be met for this plan to be viable:

1. All equipment, software and data (or their backups/failovers) are available in some manner.
2. If an incident takes place at the organization's physical location, all resources involved in recovery efforts are able to be transferred to an alternate work site (such as their home office) to complete their duties.

This plan does not cover the following types of incidents:

1. Incidents that affect customers or partners but have no effect on Reveal's systems. In this case, the customer must employ their own continuity processes to make sure that they can continue to interact with Reveal systems.
2. Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Google, Slack, and Amazon Web Services. The organization depends on such suppliers to employ their own continuity processes.

Notification List

In the event of a disaster, notify these people in order:

- Alexandre Sadones,
- Simon Bouchez

Disaster Recovery Objectives

The objectives of this plan are the following:

- Identify the activities, resources, and procedures needed to carry out Reveal's processing requirements during prolonged interruptions to normal operations.
- Identify and define the impact of interruptions to Reveal systems.
- Assign responsibilities to designated personnel and provide guidance for recovering Reveal operations during prolonged periods of interruption to normal operations.
- Ensure coordination with other Reveal 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. Please see Reveal's critical contacts on Reveal's Business Continuity Plan.

Defining Critical Systems and Services

From a disaster recovery perspective, Reveal defines two categories of systems:

Non-Critical Systems. These are all systems not considered critical by the definition below. These systems, while they may affect the performance and overall security of Critical Systems, do not prevent Critical Systems from functioning and being accessed appropriately. Non-Critical Systems are restored at a lower priority than Critical Systems. Examples of Non-Critical Systems include analytics servers.

Critical Systems. These systems host application servers and database servers or are required for the functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.

The following services and technologies are considered to be critical for Reveal business operations, and must immediately be restored (in priority order):

1. Production infrastructure
2. Transit infrastructure
3. Build and deployment infrastructure

General Disaster Recovery Plan

While specific playbooks are available for specific scenarios, there are overall rules of engagement whenever a disaster incident needs to be opened.

Notification Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Reveal. The notification sequence is listed below:

1. The first person to report the disaster should notify Alexandre Sadones.
2. Alexandre Sadones is to notify team members referenced above in the Notification List section.
3. Based on the damage assessment, if Reveal will be unavailable to customers for more than 12 hours Alexandre Sadones will declare that a disaster has occurred and that the Disaster Recovery Procedure has been activated. Alexandre Sadones also has the discretion to activate the Disaster Recovery Procedure based on other criteria.
4. In the event customer data has been compromised, customers must be notified no later than 48 hours after the incident is reported.
5. Once the Disaster Recovery Procedure has been activated, Alexandre Sadones should notify relevant personnel and executive leadership on the general status of the incident. Notification can be conducted over chat, email or phone. Alexandre Sadones may also notify the Reveal operations team if the disaster involves the Reveal premises or is related to Reveal employees.
6. If the Disaster Recovery Procedure has not been activated, the Recovery and Reconstitution phases will not be performed. Instead, Alexandre Sadones and necessary team members will perform all appropriate tasks under Reveal’s Incident Response Plan.
7. Either Alexandre Sadones or someone they select will document who was contacted and when, and will summarize each call.

Recovery Phase

This phase covers the recovery of the application at an alternate site. If the disaster involves both Critical Systems and Non-Critical Systems, the Reveal CTO may prioritize the recovery of Critical Systems and proceed to the Reconstitution Phase for the Critical Systems before Non-Critical Systems have completed the Recovery Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Assess damage to affected environments, prioritizing critical systems first. Document observations.
2. If possible, back up the affected environments in a forensically sound manner. Do not alter affected systems and applications in any manner.
3. Verify that previous backups of critical databases and systems recovery points are available before moving on to the Reconstitution Phase.

Reconstitution Phase

This phase consists of activities necessary for restoring Reveal operations to the original operating state (or permanently move operations to the new site or state, if necessary). If the disaster involves both Critical Systems and Non-Critical Systems, the Reveal CTO may prioritize reconstituting the Critical Systems before beginning reconstitution of the Non-Critical Systems. This phase consists of the following tasks, some of which can be run in parallel:

1. Begin replication of new environment using previously confirmed backups using automated and previously tested scripts.
2. Reveal utilizes multiple availability zones; however, if the primary region is unavailable replicated backups should be used to create a production environment in the failover region.
3. Test new environment using pre-written tests.
4. Test logging, security and alerting functionality.
5. Verify that systems are appropriately patched and up to date.
6. Deploy new environment to production.
7. Update DNS to new environment.

Forensics Phase

This phase consists of activities related to finding out the cause of the disaster, in cases where it is not immediately apparent. Upon the disaster incident being addressed, with customer data and Reveal operating infrastructure recovered and restored, it is appropriate to start the Forensics Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Ensure all logs from all systems, applications and databases involved in the incident have maintained their integrity in the centralized log repository.
2. If some logs did not reach the central log repository, ensure that missing system, database and application logs are retrieved. Pay attention to time keeping and clock settings, so logs from different sources can be reconciled.
3. If applicable, transfer data to a log analyzer or test instance.
4. Target network, system, and user action logs for analysis. Analyse all logs manually or with tools, tests, and scripts that have already been previously tested.
5. Document all significant findings in the timeline.

Retrospective Phase

A retrospective of an event such as a disaster recovery incident allows for all parties to understand what happened in a clear and blame-free manner. A retrospective meeting should occur within 48 hours after such an incident has occurred.

1. All relevant parties and system owners should be identified and invited to a retrospective meeting.
2. A draft agenda and disaster timeline should be sent to everyone before the retrospective meeting.
3. Retrospectives are best facilitated with an unbiased third party who was not involved with working the incident. The facilitator should ask questions of meeting participants to illuminate the severity, impact, and any follow-ups.
4. Document the retrospective meeting.
5. Produce an incident report from the retrospective agenda, timeline, and meeting notes.

Reenactment / Test Phase

Unanticipated disasters are unlikely to have documented steps for resolution. Once an unanticipated incident concludes, it should be reenacted to analyze and document how to better respond in the future. If applicable:

1. Run a simulation of the event, as understood by the retrospective meeting notes, timeline, and report. The simulation can be run with people involved or uninvolved with the disaster.
2. While running the simulation, a pre-assigned note taker should write down ideas to prevent and mitigate a similar event.
3. After the reenactment, a new and specific disaster recovery procedure should be created.

Specific Recovery Procedures

References to Disaster Recovery Plans and playbooks for restoring or failing over specific critical systems:

https://Sahrework.atlassian.net/wiki/spaces/SA/pages/721387655/Disaster+Recovery+Plan

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Reveal management will determine how serious an employee’s sense is and take the appropriate action.

Responsibility

The CTO is responsible for ensuring this policy is followed.

Last updated: *07/01/2022*