14721 Califa St.
Los Angeles, CA 91411

DISASTER RECOVERY POLICY & PLAN

The FloQast Disaster Recovery Plan ("DRP") establishes procedures to recover FloQast 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.

DISASTER RECOVERY POLICIES

- Starting from the point a disaster has been declared, the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for FloQast's Accounting Workflow Automation Software are as follows
    - RTO - 24 hours
    - RPO - 1 hour
- FloQast performs testing of the 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:

- All equipment, software and data (or their backups/failovers) are available in some manner.
- 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:

- Incidents that affect customers or partners but have no effect on FloQast's systems. In this case, the customer must employ their own continuity processes to make sure that they can continue to interact with FloQast systems.
- 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:

- Cullen Zandstra
- Erik Graham-Smith
- Mike Whitmire
- Chris Sluty
- Relevant Product Managers
- Relevant Engineering Managers
- Vicky LeVay
- Adam Schall
- Jim Fazzone

DISASTER RECOVERY OBJECTIVES

The objectives of this plan are the following:

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

DEFINING CRITICAL SYSTEMS AND SERVICES

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

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.

- Production infrastructure
    - AWS based services
    - MongoDB

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

- Build and deploy infrastructure
    - GitHub
    - Jenkins

Non-Critical Systems

These are all systems not considered critical by the definition above. 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.

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 FloQast. The notication sequence is listed below:

- The first person to report the disaster should notify Engineering Management.
- Responsible Engineering Manager is to create a P0 ticket if one has not yet been created, and create an associated Slack channel
- If and when it is confirmed that the incident impacts multiple-customers, the team members referenced above in the Notification List section are to be added to the Slack channel
- The Product Manager is to ensure the FloQast status page is updated
- Based on the damage assessment, if FloQast will be unavailable to customers for more than 24 hours Responsible Engineering Manager will declare that a disaster has occurred and that the Disaster Recovery Procedure has been activated. Responsible Engineering Manager also has the discretion to activate the Disaster Recovery Procedure based on other criteria.
- The General Counsel is to execute an investigation plan to assess the company's legal risk, and use that plan to guide the remaining activities as needed to effectively reduce litigation exposure.
- In the event customer data has been compromised, customers must be notified no later than 72 hours after the incident is reported.
- Once the Disaster Recovery Procedure has been activated, Responsible Engineering Manager should notify relevant personnel and executive leadership on the general status of the incident. Notification can be conducted over chat, email or phone. Responsible Engineering Manager may also notify the FloQast operations team if the disaster involves the FloQast premises or is related to FloQast employees.
- If the Disaster Recovery Procedure has not been activated, the Recovery and Reconstitution phases will not be performed. Instead, Responsible Engineering Managerand necessary team members will perform all appropriate tasks under FloQast's Incident Response Plan.
- Either Responsible Engineering Manager 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 FloQast 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:

- Assess damage to affected environments, prioritizing critical systems first. Document observations.
- If possible, back up the affected environments in a forensically sound manner. Do not alter affected systems and applications in any manner.
- 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 FloQast 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 FloQast 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:

- Begin replication of the new environment using previously confirmed backups using automated and previously tested scripts.
- FloQast 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.
- Test the new environment using pre-written tests.
- Test logging, security and alerting functionality.

- Verify that systems are appropriately patched and up to date.
- Deploy the new environment to production.
- Update DNS to the 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 FloQast 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:

- Ensure all logs from all systems, applications and databases involved in the incident have maintained their integrity in the centralized log repository.
- 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.
- If applicable, transfer data to a log analyzer or test instance.
- Target network, system, and user action logs for analysis. Analyze all logs manually or with tools, tests, and scripts that have already been previously tested.
- Document all significant endings 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 seven days after such an incident has occurred.

- All relevant parties and system owners should be identified and invited to a retrospective meeting.
- A draft agenda and disaster timeline should be sent to everyone before the retrospective meeting.
- 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.
- Document the retrospective meeting.
- 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:

- 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.
- While running the simulation, a pre-assigned note taker should write down ideas to prevent and mitigate a similar event.
- 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:

n/a

DISCIPLINARY ACTION

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

RESPONSIBILITY

The CTO is responsible for enforcement of this policy.

The DevOps Engineering Manager is responsible for implementation and management of this policy.

The General Counsel is responsible for approving the establishment, amendment and revocation of this policy.

CHANGE HISTORY

Finalized: 2/28/2021

Annual review: 8/26/2021

Annual review: 8/11/2022