Draup

Business Continuity and Disaster Recovery Policy

Business Continuity Plan

Objective

The objective of this business continuity plan is to prepare Draup in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible within an acceptable time frame.

Scope

The scope of this plan is limited to business continuity and disaster recovery of Draup 's production infrastructure.

Plan Objectives

- Serves as a guide for the recovery teams of Draup .
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing, and reviewing recovery procedures.

Assumptions

- Key people (team leaders or alternates) will be available following a disaster.
- A national disaster such as a nuclear war is beyond the scope of this plan.
- This document and all vital records are stored in a secure off-site location and not only survive the disaster but are accessible immediately following the disaster.
- Each support organization will have its own plan consisting of unique recovery procedures, critical resource information, and procedures.

Disaster Definition

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by Draup operations. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

Preparation for Disaster Recovery & Business Continuity

- It is essential that frequent backups are taken, and backups are stored at a redundant location to facilitate restoration in case of a disaster.
- A backup restoration exercise should be performed by the Infra Operations Person with help from the engineering team.
- The Information Security Officer should ensure that a disaster recovery mock drill is conducted by the Engineering team, which will then allow them to invoke this plan effectively. This exercise may be a tabletop exercise based on

the availability commitments.

- If required, through the disaster recovery exercise, the Engineering team should evaluate the following:
    - Recovery time objective
    - Recovery point objective

Instructions for Using the Plan

Invoking the Plan

This plan becomes effective when a disaster occurs.

Disaster Declaration

The Information Security Officer and/or Engineering Head is responsible for declaring a disaster and activating the various recovery teams as outlined in this plan.

In a major disaster situation affecting multiple business units, the decision to declare a disaster will be determined by senior management. The Engineering Team will respond based on the directives specified by senior management.

Plan Review & Maintenance

This document and the disaster recovery mock drill must be reviewed at least once annually.

Notification of Incident/Disaster

- In cases of technical incidents, the Infra Operations Person/On-Call Engineer personnel should contact the Information Security Officer.
- For any operational incident, it is the responsibility of the user/employee to report it as soon as possible through like e-mail or telephone, as applicable.
- The Information Security Officer should be notified promptly when any of the following conditions exist:
    - Any server is down for three or more hours.
    - Any problem at any system that would cause the above condition to be present or there is a certain indication that the above condition is about to occur.
- The Information Security Officer should contact the respective Draup Business heads and report that a disaster has taken place.
- Once a disaster has been declared, it must follow the incident management procedure and change management procedures while trying to bring back the availability of services.
- Declare a disaster only if the situation is not likely to be resolved within predefined time frames. The person who is authorized to declare a disaster must also have at least one backup person who is also authorized to declare a disaster in the event the primary person is unavailable.
- It is the responsibility of the Information Security Officer to ensure the event of a disaster and the successful recovery are communicated to relevant stakeholders, customers, and regulatory bodies as applicable.

Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

Disaster Recovery Policy

Draup ’s Disaster Recovery Policy outlines the guidelines, procedures, and workarounds to follow in case of a disaster strikes. A few examples of disasters are the failure of power supply, failure of telecommunications, social unrest, terrorist attacks, fire, or natural disasters.

Scope

Draup relies largely on cloud vendors to provide its services. Its production infrastructure is completely hosted with cloud-based providers. Consequently, there are two primary implications of disasters:

1. Our primary infrastructure provider for production services has degraded service or is unavailable. Specifically, one of their hosting regions has degraded services.

2. Our primary office(s) location is partially or completely unavailable as a place for our staff to work safely and effectively.

Since Draup relies mostly on cloud services, most of its core operations can be carried out even if staff members cannot reach their office(s). It suffices for staff members to have access to their laptop and an internet connection to carry out their basic job functions in order to keep our customer services uninterrupted. The advantage of Draup ’s workforce is that if there are clusters of people or systems that are unavailable, the rest of the company will continue to operate normally.

As a result, the remainder of this Disaster recovery policy details steps to follow in the event where our primary production infrastructure is unavailable.

Assumptions

This plan assumes that the following requirements are satisfied:

1. Critical data backups are available (as covered in our Data Backup Policy)
2. Our infrastructure provider[s] has multi-region support, and at least one of their worldwide regions is unaffected by the disaster.

3. Incidents that affect our customers or partners but have no effect on our systems are handled by their own respective business continuity and disaster recovery plans.

Priority

Consider the following priority order in restoring our production systems.

1. Critical systems like application servers, background workers, and database servers are the bare minimum requirements for a functioning production system. 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.

2. Non-Critical Systems like analytics, monitoring, logging, etc do not prevent critical Systems from functioning and being accessed appropriately. Non-Critical Systems are restored at a low priority.

Disaster Recovery Plan

Disaster recovery includes the following steps

Is the event a disaster?

1. As a guiding principle, if our systems are going to be unavailable for more than 24 hours, we may have to activate our disaster recovery plan.

2. The first person to recognize a disaster should notify the CEO. The CEO will consider the information available and decide if the situation warrants activation of the Disaster Recovery Plan, or if it can be handled more appropriately under the Incident Response plan. The CEO may also decide to activate the Disaster Recovery Plan based on other criteria.

Assign a Team

If the Disaster Recovery Plan has been activated, the CEO will appoint a team of one or more people to carry out subsequent steps. The CEO will choose the team depending on the type of disaster, the nature of affected systems, availability of staff while giving priority to staff who have performed prior disaster recovery tests.

Recovery Groundwork

1. The team should assess if the disaster affected both Critical and Non-Critical Systems. In such cases, the team should prioritize the recovery of Critical Systems and proceed to the next steps before addressing the non-critical systems.
2. The team should analyze damage to affected environments. If possible, it should back up persistent parts of the system (like databases).

3. Overall, the team should verify that previous backups of critical data are available before moving on to the next steps.

Recovery

1. Our infrastructure provider[s] supports multiple regions and availability zones. If the primary availability zone or a region is unavailable, pick another availability zone/ region with similar functionality for subsequent steps.
2. Begin building a new environment using the steps followed during Disaster recovery testing. These steps may be available in a runbook. Also, use the database backups as confirmed in the steps above.
3. Test the new environment to check if all critical functionality is working as expected (for instance, login, logout, dashboard, etc).
4. Make the new environment live for your customers if everything seems okay. Watch closely for unexpected bugs or outages for 24 hours.

5. The management team should decide if the new environment is a temporary setup or should it continue indefinitely as a primary environment. If the new environment continues to be the primary environment, ensure that all backups and other non-critical functionality like monitoring, etc are configured correctly.

Postmortem

1. After the disaster incident is addressed and all functionality in the production system is stabilized, the team should analyze the root cause of the disaster if it is not obvious.
2. Analyze the available logs, databases, etc to learn more information about potential causes.
3. The team should document all learnings from the incident, update the runbooks if any, and share the learnings with relevant Draup staff.

4. Draup management should communicate relevant details of the incident internally. In the event customer data has been compromised, customers must be notified.

Periodic testing

To ensure our ability to execute this plan effectively, the disaster recovery plan is periodically tested.

Specifically, we perform the following tests:

1. Restore critical data backups created as per our data backup policy.

2. Tabletop review of this Disaster recovery plan Please refer to our Process Configuration for the frequency of these tests.

Non-Compliance

Draup staff who violate this policy may face repercussions in proportion to the impact of their violation. Draup management will determine how serious a staff member’s offense is and decide the appropriate penalty. Penalties may include a warning (oral/written) or suspension or termination for more serious offenses.

Questions

If you have any questions regarding this policy, please reach out to the policy owner.

Business Continuity and Disaster Recovery Policy

Version	v1
Created By	Scrut Team, Mar 17, 2025
Approved By	Kashish, Apr 1, 2025
Published By	Kashish, Apr 1, 2025