Disaster Recovery Plan (DRP)

MDY-BCP-PLN-02

Code	MDY-BCP-PLN-02
Version	2.5
Date of Version	March 2025
Created by/Updated by:	GRC Team Lead (name removed)
Approved by:	VP R&D (name removed)
Confidentiality Level	For External Use

Table of Contents

1. Purpose & Goals

The purpose of this plan is to identify disasters (as defined below) as quickly as possible to minimize the impact on the Company and its customers, and to restore core operations as soon as possible and no longer than the declared RTO in this policy.

Accordingly, the policy's goals are:

- Preventing, as possible, and limiting the extent of disruption and damage to the Company's core service operations
- Providing smooth and rapid restoration of core service service
- Establishing alternative means of operation in advance
- Training personnel on emergency procedures
- Minimizing the financial impact of the interruption

2. Scope

- monday.com manages and delivers its services using AWS.
- monday code and WorkCanvas manage and deliver their services using GCP.

3. Disaster Recovery Teams & Responsibilities

- Full details on roles and responsibilities of the Disaster Recovery Team (DRT) is in **Appendix A**.
- General:
  - Each DRT member will designate an alternate.
  - All DRT members and their alternates shall have access to an updated contact list of the DRT's phone numbers and internal communication tool in the Company, as detailed in **Appendix B**.
  - Infrastructure leadership must have access to this plan in the company's organizational Policies Portfolio (in multiple sources).
  - All DRT members should familiarize themselves with the contents of this plan.

4. Disaster Declaration

The Event Manager, with input from the DRT, is responsible for declaring a disaster and activating the various recovery teams as outlined in this policy. Any of the following events will be declared as a disaster:

- The service is not available for at least 10% of our customers.
- A core feature or component in the system is down.
- A primary workflow within the system is disrupted.

For cyber threats, refer to the Information Security & Data Incident Response Procedure.

For disaster that has to do with monday.com employees, offices and facilities (e.g: inability to attend the offices, lack of employees availability, electricity or internet problems), refer to Business Continuity Plan.

5. Disaster Management

- The DRT shall contact the Event Manager and provide the following information when any of the following conditions apply:
    - Any problem with any system or location that would cause any of the conditions listed above in section 4 to be present,
    - or if there is an indication that the above condition is likely to occur.
- The DRT will provide the following information: type of disaster, and summary of the damage (e.g., minimal, heavy, total destruction).
- Based on the information above, the Event Manager needs to decide how to respond to the event. If a disaster is not declared, the team will continue to address and manage the situation and provide periodic status updates to the Event Manager. If a disaster is declared, the Event Manager will decide on the next steps, while the DRT will continue to work to solve the disaster.
- The Event Manager will contact the VP of Customer Success, PR, Legal, Security and Investors Relations and report if a disaster has taken place.

6. Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

In a case of disaster, the Company's Recovery Time Objective (RTO) is 24 hours.

In a case of disaster, the Company's Recovery Point Objective (RPO) is 12 hours.

7. External Communications & Vendors

- monday.com Public Relations (PR) department are designated as the principal contacts with customers, media, and other external organizations.
- monday.com's Legal Team is designated as the principal contact with legal authorities.
- The DRT will be responsible for contacting relevant vendors as soon as the disaster is declared. The list is available for monday.com's employees in the Contacts - Critical Systems board which is managed by the IT team.

8. Data and Backups

monday.com utilizes AWS backup services, and monday code and WorkCanvas utilize GCP backup services to manage and perform backup tasks on various types of service-related data retained within the production environment, to enable the availability and redundancy of data.

In the production environment, every DB has at least one replica for performance and redundancy purposes. The databases and critical portions of the application file systems for monday.com, monday code, and WorkCanvas are backed up daily. Backup data is retained for 25 days in the local region and 7 days in a geographically diverse location. Access to these backups is restricted to authorized individuals only.

9. DR Security Assessment

In the specific case of a security breach of monday.com's systems or environment, a security breach assessment will be performed by monday.com's CISO to assess the parts of the system being affected.

10. Policy Review and Testing

This plan must be reviewed annually and tested at least twice a year. The test may be in the form of a walk-through, mock disaster, or component testing.

Note: Internal Appendixes have been redacted from this version