Disaster Recovery Plan (DRP)

MDY-BCP-PLN-02

Code	MDY-BCP-PLN-02
Version	2.4
Date of Version	February 2024

Table of Contents

1. Introduction

This Disaster Recovery Plan (DRP) captures, in a single repository, all of the information that describes the steps that monday.com (**"monday.com"** or **"the Company"**) should take in order to recover from a Disaster (as described below).

2. Purpose

The purpose of this plan is to identify disasters as quickly as possible to minimize 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 document. Accordingly, the plan's goals include:

- Limiting the extent of disruption and damage.
- Minimizing the economic impact of the interruption.
- Establishing alternative means of operation in advance.
- Training personnel regarding emergency procedures.
- Providing smooth and rapid restoration of service.

To emphasize, as possible, the primary purpose of this plan is to prevent or minimize the risks for an occurrence of a Disaster.

3. Scope

The scope of this plan is monday.com's production operations that affect customers' experience and data.

Non-production services, personnel, HR and real estate disasters are out of scope of this plan. Mitigation of other disaster types is addressed in monday.com's **Business Continuity Plan (MDY-BCP-PLN-01)**.

A national disaster such as nuclear war is beyond the scope of this plan.

4. Assumptions

- Key personnel (team leaders, tech leads or alternates) will be available following a disaster;
- This policy document is stored in a secure highly redundant shared folder and not only survives the disaster but is accessible immediately following the disaster.
- The company will have one general plan consisting of unique recovery procedures, critical resource information and procedures.

5. Recovery Teams

- Event Manager
- Disaster Recovery Team (DRT)

Note: See **Appendix A** for details on the roles and responsibilities.

6. Team Member Responsibilities

- Each team member will designate an alternate.
- All members and their alternates should have access to an updated contact list of their team members' phone numbers;
- All team members should have access to this plan in the company's organizational Policies Portfolio in case the disaster happens after normal work hours;
- All team members should familiarize themselves with the contents of this plan.

7. 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 plan. 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.

A disaster will be declared if the situation is not likely to be resolved within predefined time frames. The person who is authorized to declare a disaster should also have at least one alternate who is also authorized to declare a disaster in the event the primary person is unavailable.

8. Invoking the Plan

This plan becomes effective when a disaster occurs. Problem management procedures will be initiated and remain in effect until normal operation is declared.

9. Recovery Time Objective (RTO)

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

10. Recovery Point Objective (RPO)

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

11. External Communications

monday.com Public Relations (PR) personnel 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.

12. Communicating with Vendors

The DRT will be responsible for contacting relevant vendors as soon as the disaster is declared.

13. Crucial Vendors - Contact Details

The list is available for monday.com's employees in the organizational file repository.

14. Data and Backups

monday.com and AWS backup services are responsible for managing and performing backup tasks on various types of service-related data retained within the production environment to enable availability and redundancy of data. In the production environment, every DB has at least one replica for performance and redundancy purposes. The monday.com application database and critical portions of the application file systems are backed up daily. 25 days of backup data is kept in a geographically remote location. Access to the backup is restricted to authorized individuals.

15. DR Security Assessment

In the specific case of a security breach of monday.com's network systems, a security breach assessment will be performed by monday.com's CISO (refer to **Appendix B**) to assess the parts of the system being affected.

16. Plan Review and Maintenance

This plan must be reviewed annually and exercised on a biannual basis. The test may be in the form of a walk-through, mock disaster, or component testing. Additionally, with the dynamic environment present within monday.com, it is important to regularly review the listing of personnel and phone numbers contained within the plan.

17. Providing Status to Event Manager

The DRT should contact the Event Manager and provide the following information when any of the following conditions apply: (see **Appendix B** for contacts list)

- Any problem with any system or location that would cause any of the conditions listed above in section 7 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 , summary of the damage (e.g., minimal, heavy, total destruction);
- The Event Manager will contact the VP of Customer Success and report if a disaster has taken place.

18. Decide on the Course of Action

Based on the information obtained by the DRT, 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.