Disaster Recovery Plan

Table of Contents

Overview

The Vercel Disaster Recovery Plan (DRP) establishes procedures to recover Vercel operations following a disruption resulting from a disaster affecting Vercel production environments. The types of disasters contemplated by this Plan include, but are not limited to, natural disasters, political disturbances, man-made disasters, external human threats, and internal malicious activities.

Scope

This Plan includes all resources and processes necessary for service and data recovery and covers all information security aspects of business continuity management. In the event of an actual emergency, this Plan may be modified to ensure the physical safety of all individuals performing work for or on behalf of Vercel including Vercel employees and contingent workers, contractors, consultants, contingent, temporary and other workers supporting Vercel business operations, and any other entities permitted to act on behalf of or in representation of Vercel (collectively as referred to as "Personnel"), systems, and data. From a disaster recovery perspective, Vercel defines two categories of systems within the Integrated Management System (IMS):

- **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 restoration process initiated, immediately upon becoming unavailable. The following services and technologies are considered to be critical for Vercel business operations, and must immediately be restored (in priority order):
    1. Hosting platform infrastructure
    2. Production infrastructure
    3. Build and deployment infrastructure
- **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.

This Plan does not cover the following types of incidents:

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

- Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Google Cloud, Microsoft Azure, Github, and Amazon Web Services. Vercel does not extend incident response (IR) efforts to third parties, but will rely on third party IR efforts and monitor through status pages, emails and direct updates.

Objectives and Goals

The principal objective of this Plan is to develop, test, and document a clear and structured plan to help designated Vercel Personnel understand and recover as quickly and effectively as possible from an unforeseen disaster or emergency that disrupts systems and/or business operations.

Questions?

If you have additional questions on this Plan, please reach out to the Security team at security@vercel.com or #help-security in Slack.

Change Record

Document Name	Disaster Recovery Plan
Document ID	PLAN-003
Plan Owner	Talha Tariq
Title	Chief Technology Officer, Security
Digital Signature	
Effective Date	May 22, 2026

Ver.	Date	Reviewer(s)	Description of Change

6.0	May 22, 2026	**People** [redacted] **Finance** [redacted] **Security** [redacted]	Annual refresh; updated contact details in Appendix B
5.0	April 2025	**Information Security Steering Committee** [redacted] **Security** [redacted]	Updated contact information and associated offices
4.0	June 6, 2024	**Information Security Steering Committee** [redacted] **Security** [redacted]	Minor updates to reflect physical office space

3.0	May 25, 2023	**Information Security Steering Committee** [redacted] **Security** [redacted]	Updates to phases and process changes; addition of Appendix B
2.0	May 30, 2022	**Information Security Steering Committee** [redacted] **Engineering** [redacted] **IT** [redacted] **Information Security** [redacted] **Privacy Team** [redacted]	Focused purely on the Production environment, while all business and ops functions are shifted to the Business Continuity & Crisis Management Plan. Moved to new template, updated roles/responsibilities references, adjusted language.
1.0	Sept 7, 2020	[redacted]	Original Policy

Appendix A - Examples

Natural	Human Caused
Avalanches	Civil Disorder
Earthquakes	Cyber Attacks (DDoS, RCE, Data Theft, etc.)
Floods	Explosions
Fires	Hazardous Chemical Spills
Heat Waves	Human Transmitted Viruses
Land/Mud Slides	Fires (Accidental / Arson)
Naturally Occurring Viruses	Political or Civil Unrest (Riots)
Solar Flares	Structural Failures
Storms	Terrorism, Tyranny
Tsunamis	Vehicular Accidents
Tornados	Water Contamination
Volcanic Eruption	War

Appendix B - External Contacts

Contact	Phone / Email	Additional Information
Insurance	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]