Security Incident Response Plan

Table of Contents

Overview

Vercel is committed to maintaining the security and privacy of our customers. This Plan focuses on Vercel's procedure for responding to incidents discovered within Vercel's environment.

Each incident is unique, but the purpose of this document is to outline the steps necessary to address an incident at Vercel. Due to a unique level of technical expertise across all teams at Vercel, the Security team may not interact with all incidents created internally. When addressing incidents there are three main things to keep in mind: timely communication, comprehensive documentation, and scoped investigation.

Scope

This Plan applies to all individuals performing work for or on behalf of Vercel, including full-time employees, contractors, consultants, contingent, temporary and other workers (collectively referred to as "Personnel"), and any systems, applications, or integrations where information and data is stored, transmitted, processed, or disposed.

Incidents related to Vercel's Integrated Management System (IMS), malware on endpoints, malicious internal employee actions, ransomware, exposure or abuse of AI models or improper inferences, prompt injection, and public-facing security breaches are all examples of incidents affected by the scope of this document.

This Plan does not supersede any other applicable law or higher-level company directive or existing labor management agreements in effect as of the effective date of this Plan.

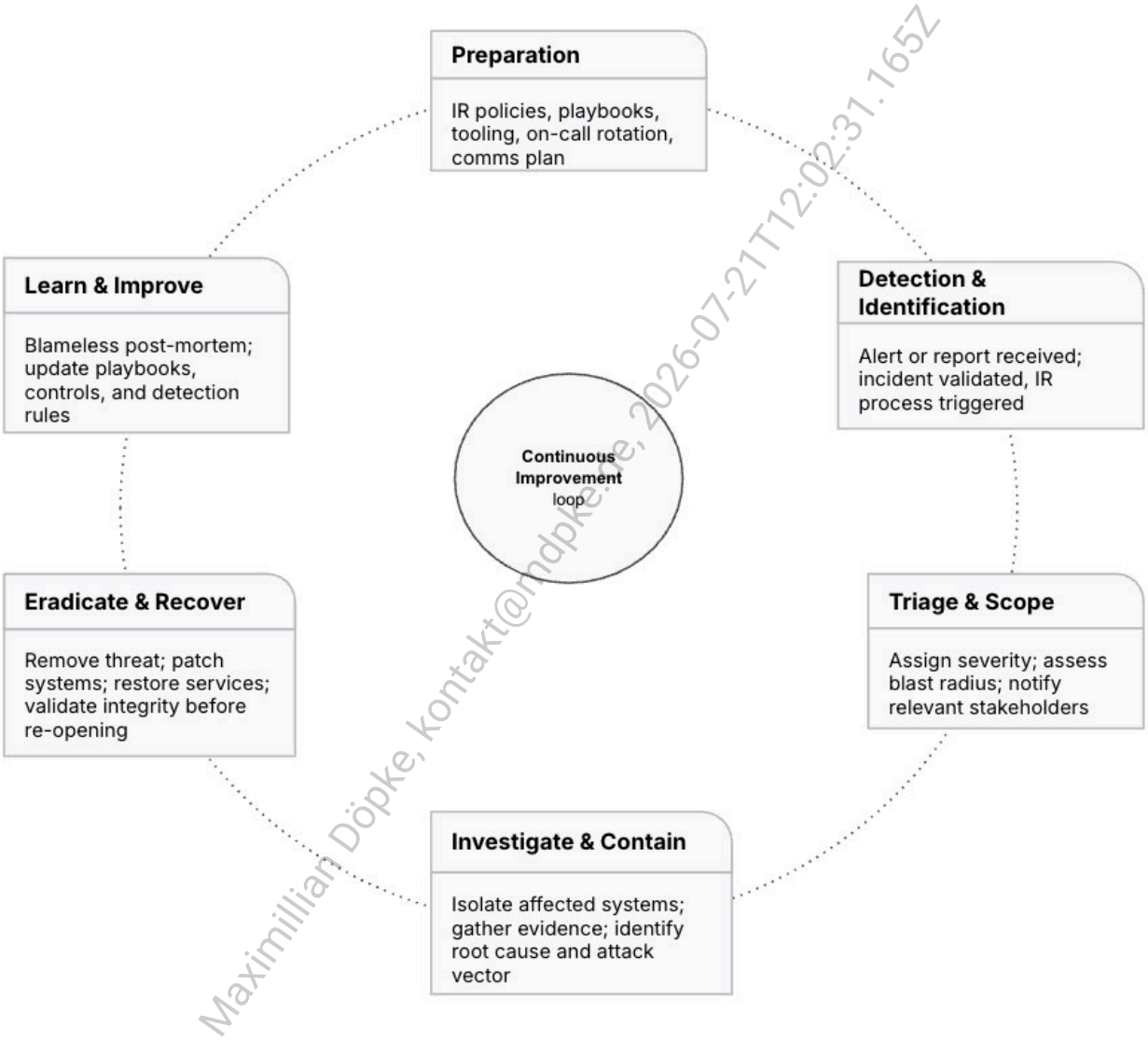
Compliance

Any Vercel user found to have violated this Plan or any policy, standard, or procedure may be subject to disciplinary action, up to and including termination of employment. Vercel management will determine how serious a Personnels offense is and take the appropriate action. Violators of local, state, federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Incident Response Process

Vercel's Security and Engineering teams handle many incidents internally. System owners regularly fix issues as they arise, often not creating a formal incident. Communication

between Security, Engineering, and other stakeholder teams (i.e., Legal) is paramount for successful incident declaration, creation, and triage. The Security team will be involved in any incidents related to the security, confidentiality, and availability of Vercel systems, environments, or infrastructure and any impact to Personnel or customer data, regardless of determined size of incident.



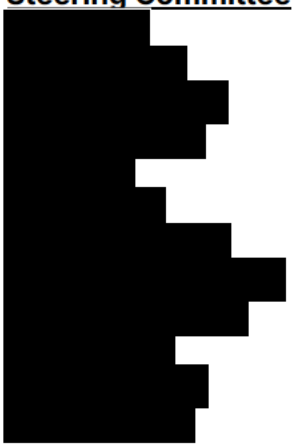
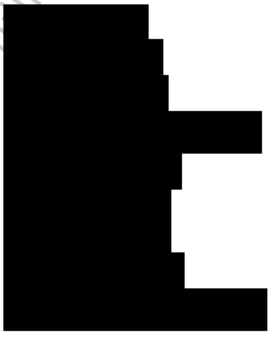
Questions?

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	Security Incident Response Plan
Document ID	PLAN-001
Document Owner	Talha Tariq
Title	Chief Technology Officer, Security
Digital Signature	
Effective Date	May 22, 2026

Version	Date	Reviewer(s)	Description of Change
6.0	May 22, 2026	**Security** [redacted]	Updated to align with NIS2 Directive and ISO 42001 requirements; updated forensic and incident investigation third parties; updated incident response lifecycle to align with NIST standards
5.0	April 22, 2025	**Information Security Steering Committee** [redacted] **Security** [redacted]	Updated incident response (Appendix D) to include latacora information, added SRE Runbooks link.

4.0	February 21, 2024	**Information Security Steering Committee**  **Security** 	Updated to align with HIPAA requirements
3.0	May 25, 2023	**Information Security Steering Committee**  **IT**  **People Team** 	Updated descriptions to align with process enhancements and tooling updates. Modified to include ISO 27001:2013 standards.

		Engineering [redacted]	
2.0	June 12, 2022	Engineering [redacted] Information Steering Committee [redacted] Security [redacted] IT [redacted] Privacy [redacted]	Migrated old IRP into this document, modernized approach to incident response. Added scope, incident response steps, visuals on incident ownership, incident retainer information, international contact points.
1.0	Sept 7, 2020	[redacted]	Original Policy