INFORMATION SECURITY POLICY

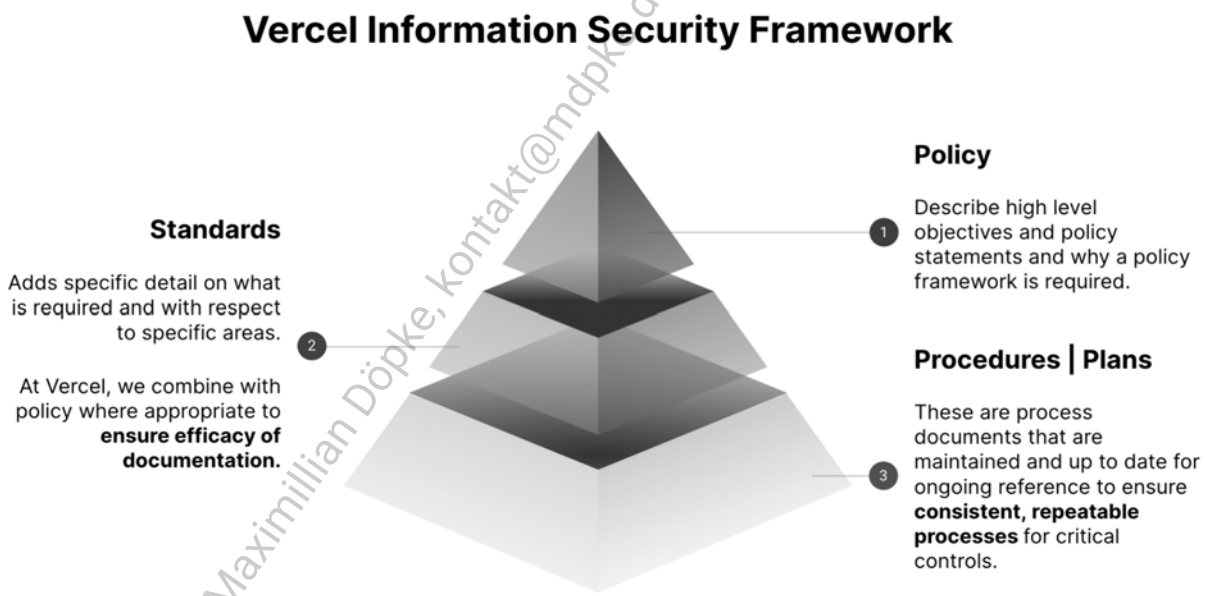
Table of Contents

Overview

Vercel, Inc. is a global organization committed to protecting the safety, security, and privacy of its people, processes, technology, and customers. This Information Security Policy and Integrated Management Systems (IMS)[1], establishes measures to ensure the confidentiality, integrity, availability, reputation, and overall safety of the company.

An effective security program requires collaboration, participation, and support from all Vercel personnel and entities associated with Vercel. This Policy forms the foundation for process, controls, procedures, and plans that Vercel implements and operates to meet its commitments.

As a result, it is the responsibility of all individuals performing work for or on behalf of Vercel to be familiar with and adhere to Vercel's policies and procedures. This includes Vercel employees, contingent workers, contractors, consultants, temporary and other workers supporting Vercel business operations, and any other entities permitted to act on behalf of or in representation of Vercel (collectively referred to as "Personnel"). Vercel's Information Security Framework shall be regularly implemented, reviewed, and improved to ensure that Vercel's security objectives are met.



[1] References to Vercel's Integrated Management System (IMS) include the Information Security Management System (ISMS) and Artificial Intelligence Management System (AIMS) which are inclusive of Vercel's system of internal controls and compliance framework requirements (i.e., PCI DSS, SOC 2, ISO 27001, ISO 42001, etc.).

Scope

This Policy applies to all Vercel Personnel and any systems, applications, or integrations where Vercel information and data is stored, transmitted, processed, or disposed. This Policy 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 Policy.

Vercel's legal addresses include:

- Vercel Inc. (USA): 440 N Barranca Ave #4133 Covina, CA 91723
- Vercel GmbH (Germany): Tiniusstraße 29 b, 13089 Berlin, Germany
- Vercel UK Ltd (London): 4th Floor, St. James House, St. James Square, Cheltenham, England, GL50 3PR
- Vercel Canada Inc.(Canada): 1200 - 925 West Georgia Street, Vancouver, BC V6C 3L2, Canada
- Vercel Japan K.K. (Japan): 36-6, Irifune 4-chome, Urayasu-shi, Chiba, Japan
- Vercel Australia Pty. Ltd. (Australia): Suite 3A16, level 14, 275 Alfred Street N, North Sydney NSW 2060, Australia (c/o Landsowne Financial Pty Ltd)

Vercel's physical office locations include:

- California (HQ): 201 MissionStreet, #3, San Francisco, CA 94105
- New York: (Industrious) 1411 Broadway, 17th Floor, Suite F, New York, NY, 10018
- Austin: (Industrious) 98 San Jacinto Blvd, Ste 400, Austin, TX 78701
- London: (Industrious) 131 Finsbury Pavement, 1st Floor, Office 01-102, London EC2A 1NT, UK
- Berlin: (Fora) - Linden Palais Unter den Linden 40, 10117 Berlin, Germany

Objectives and Goals

The primary goals of this Policy are to:

- Establish an information security framework to protect the organization's personnel, data, systems, and assets from internal and external threats
- Implement effective security and privacy controls to support Vercel's operations and IMS
- Enhance the growth, maintenance, and review of business operations and product development
- Continuously improve the IMS through data-driven metrics

Compliance

Any Vercel user found to have violated this Policy or any other policy, standard, or procedure may be subject to disciplinary action, up to and including termination of employment. Vercel management will determine how serious an employee's 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.

Policy Lifecycle

This Policy is updated annually or upon material changes to the IMS following the appropriate review and communication processes to ensure relevance and effectiveness. Updates are noted in the Change Record to highlight the pertinent changes from the previous versions. Historic artifacts are retained to track versioning and archival capabilities. The Security team owns the updates and modifications to relevant policies and compliance frameworks , while members of the Integrated Management System Steering Committee provide review and approval for changes. Additional subject matter experts shall be engaged for review and noted in the Change Record as needed.

To keep Personnel informed, updates to company policies, including the Information Security Policy and related documents, are announced to Personnel via All Hands meetings, Slack messages, or email announcements by the Security team or applicable document owner(s). Personnel may provide feedback, recommendations, or edits to Vercel's policies and procedures in the Policy & Documentation Feedback page in Notion.

Questions?

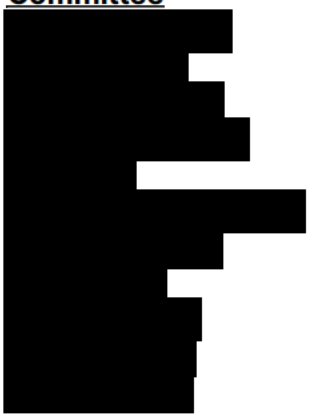
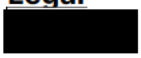
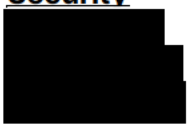
If you have additional questions on this Policy, please reach out to the Security team at security@vercel.com or #help-governance-risk-compliance in Slack.

Change Record

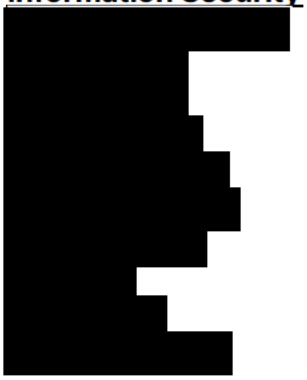
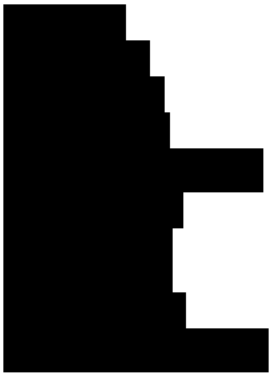
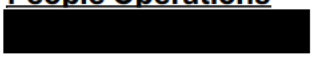
Document Name	Information Security Policy

Document ID	POL-001
Policy Owner	Talha Tariq
Title	Chief Technology Officer, Security
Digital Signature	
Effective Date	May 25, 2026

Ver.	Date	Reviewer(s)	Description of Change
6.0	May 25, 2026	**Security** [redacted] **Legal** [redacted] **People** [redacted] **Finance** [redacted]	Updates to reflect ISO 42001 requirements; changes to IMS scope; process and tool changes
5.1	August 15, 2025	**Security** [redacted] **Legal** [redacted]	Updated to include minor changes in internal operations, as well as inclusion of TISAX requirements

5.0	May 1, 2025	**Information Steering Committee**  **Security**  **Legal** 	Updates to reflect new office spaces, PCI requirements, new security vendors, data destruction SLAs, access management, password management, and risk management.
4.1	November 11, 2024	**Security** 	Updates to include new PCI requirements

4.0	June 5, 2024	**Security** [redacted] **People Operations** [redacted] **Information Security Steering Committee** [redacted]	Updates to include physical security with new HQ office space and HIPAA requirements
3.1	November 28, 2023	**Security** [redacted] **People Operations** [redacted] **Information Security Steering Committee** [redacted]	Minor updates to align with PCI DSS standards

3.0	May 25, 2023	**Information Security**   **People Operations** 	Updated to align with ISO 27001:2013 standards; ISMS governance; integration of AI; process and third party tooling updates, edits for grammar, clarity, and easier reading.

2.0	June 2, 2022	**Information Security Steering Committee** [redacted] **IT** [redacted] **Information Security** [redacted] **Privacy Team** [redacted]	Integrated Mono-Policy which incorporates Asset Management, Back-up plan, Crypto, Data Classification, Data Deletion, Password Policy, Responsible Disclosure, Risk Assessment (Add Risk Management), Systems Access Control Policy, Vendor Management, Vuln Management, SDLC Declaration as ISMS
1.0	Sept 7, 2020	[redacted]	Original Policy