ZEROMARGIN.LOANS

Security

Security practices for ZeroMargin.loans, including third-party cloud infrastructure, Google sign-in, data handling, reporting, and deletion requests.

> Update of October 3, 2026: Account sign-in, liquidity requests, and file uploads on ZeroMargin.loans are suspended. While suspended, the website does not collect personal information through these features. Information submitted earlier is kept with restricted access and can be deleted on request at info@zeromargin.loans.

EFFECTIVE DATE	VERSION	DOCUMENT ID
October 3, 2026	1.1.0	ZM-SEC-001

1.0 Security Overview

1.1 Our Approach

ZeroMargin.loans uses reasonable administrative, technical, and operational measures designed to protect website information and support the confidentiality, integrity, and availability of relevant systems and data.

This page provides a high-level overview of our current security approach. It is not a certification statement, a guarantee of specific outcomes, or a comprehensive description of all controls in place.

1.2 Current Infrastructure

At this stage, ZeroMargin.loans uses third-party cloud infrastructure, including Firebase services provided by Google, for core website hosting, authentication, database, storage, and related platform capabilities.

Sign-in through Firebase Authentication with Google is currently disabled. Request information submitted earlier remains stored using Firebase services, and access rules block new requests and uploads. We may add, replace, or migrate infrastructure over time, including use of Google Cloud, Amazon Web Services, or other cloud and operational providers.

1.3 Shared Responsibility

Security is a shared responsibility. Users are responsible for using secure devices and networks, protecting access to their Google account and devices, exercising care when submitting information, and reporting suspected security issues when identified.

Users should not submit passwords, full government identification numbers, private keys, payment credentials, or other highly sensitive information unless the website specifically requests it for a defined purpose.

2.0 Data and Access Controls

2.1 Authentication

User sign-in is currently disabled. When it was available, it relied on Google authentication through Firebase Authentication. This means account access depends in part on the security of the user's Google account, including any password, passkey, recovery, device, and two-factor settings configured with Google.

If you believe your Google account, ZeroMargin.loans account access, or submitted request information may have been accessed without authorization, contact us at info@zeromargin.loans.

2.2 Access Controls

We seek to limit access to relevant systems and customer information to authorized personnel, contractors, and service providers with a legitimate operational need.

Access practices may include role-based permissions, Firebase security rules, administrative separation between user-visible and internal request data, and review of access needs as the product evolves.

2.3 Data Storage

Request information submitted earlier is stored using Firebase services; new submissions are blocked. Submitted information may include request details, account identifiers, portfolio-related inputs, file metadata, and service workflow information needed to operate the request experience.

We aim to collect and retain only information reasonably needed for the website, request workflow, security, support, compliance, and service improvement purposes described in our public notices.

Market data shown on the website is published as part of each website release and cannot be changed through the public website.

2.4 Transport Security

Firebase Hosting and modern browsers generally use HTTPS/TLS transport protections for data transmitted between user devices, browsers, and website infrastructure.

Users should access ZeroMargin.loans through the official website and avoid submitting information over untrusted devices, compromised browsers, or public networks they do not trust.

3.0 Vendors and Third-Party Services

3.1 Cloud Infrastructure

ZeroMargin.loans currently relies on third-party cloud infrastructure, including Firebase services provided by Google. Provider controls, availability, terms, policies, and security practices are part of the operational environment for the service.

We do not control every aspect of third-party infrastructure. Outages, policy changes, security incidents, account restrictions, or technical limitations affecting third-party services may affect ZeroMargin.loans.

3.2 Other Service Providers

We may use additional third-party providers for analytics, error monitoring, communications, hosting support, security tooling, or operational workflows. We seek to use vendors that are appropriate for the nature of the service provided and the information involved.

4.0 Monitoring and Incident Response

4.1 Monitoring Practices

We may use logging, monitoring, alerting, and related operational tools to detect errors, misuse, suspicious activity, availability issues, or other events affecting website operations or security posture.

Monitoring may include technical metadata such as timestamps, request paths, browser or device information, authentication events, error messages, and other operational signals, subject to our Privacy Notice.

4.2 Incident Response

If we become aware of a security issue affecting ZeroMargin.loans, we will assess the issue, take steps we consider appropriate to contain or remediate it, and provide notices where required by applicable law or where we believe notification is appropriate.

Because the product and infrastructure are evolving, response practices may change over time as operational maturity increases.

4.3 Reporting Security Concerns

If you become aware of a suspected vulnerability, unauthorized access, misuse event, data exposure, or other security concern relating to ZeroMargin.loans, report it to info@zeromargin.loans.

Please include enough detail for us to understand and reproduce the issue where possible, but do not include sensitive personal data, credentials, private keys, or third-party confidential information in the report unless we specifically request it through a secure channel.

5.0 User Controls and Data Requests

5.1 Account and Data Requests

Users may request help with account access, submitted request information, or deletion of data associated with their use of ZeroMargin.loans by contacting info@zeromargin.loans.

We may need to verify the requester's identity or account control before acting on a deletion, access, or correction request. Some information may be retained where reasonably necessary for security, legal, fraud prevention, compliance, backup, dispute, or operational purposes.

5.2 Questions

Questions about this Security page, account access, data deletion, or security practices should be directed to info@zeromargin.loans.

6.0 Limitations

6.1 No System Is Completely Secure

No method of transmission over the internet, no digital service, no authentication system, and no storage environment can be guaranteed to be completely secure or continuously available.

While ZeroMargin.loans seeks to maintain reasonable safeguards, users should understand that residual risk is inherent in online systems and communications.

END OF DOCUMENT | ZM-SEC-001 v1.1.0