Security

High-level security safeguards and incident handling practices for ZeroMargin.loans.

EFFECTIVE DATE	VERSION	DOCUMENT ID
March 21, 2026	1.0.0	ZM-SEC-001

1.0 Security Overview

1.1 Our Approach

ZeroMargin.loans seeks to use 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 general security approach. It is not a certification statement, a guarantee of specific outcomes, or a comprehensive description of all controls in place.

1.2 Shared Responsibility

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

2.0 Administrative and Technical Safeguards

2.1 Access Controls

We seek to limit access to relevant systems and information to authorized personnel, contractors, and service providers with a legitimate business need, subject to internal access management practices and role-based considerations where appropriate.

2.2 Encryption in Transit

Where appropriate, we seek to use industry-standard transport protections for data transmitted between user devices, browsers, and website infrastructure.

This section should be refined once the final production infrastructure and implementation details are confirmed.

2.3 Vendor and Infrastructure Controls

We may rely on third-party hosting, infrastructure, analytics, communications, and operational vendors. We seek to select vendors using reasonable diligence and to rely on contractual, technical, and operational safeguards appropriate to the nature of the service provided.

3.0 Monitoring and Incident Response

3.1 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.

3.2 Reporting Security Concerns

If a user becomes aware of a suspected vulnerability, misuse event, or other security concern relating to ZeroMargin.loans, the issue should be reported to the designated security contact.

This section remains a placeholder until the production reporting channel is finalized.

4.0 Limitations

4.1 No System Is Completely Secure

No method of transmission over the internet, no digital service, and no storage environment can be guaranteed to be completely secure. While ZeroMargin.loans seeks to maintain reasonable safeguards, users should understand that residual risk is inherent in online systems and communications.

5.0 Contact

5.1 Security Contact

Questions regarding this Security page or reports of possible security issues should be directed to the designated security contact for ZeroMargin.loans once that contact channel is finalized.

END OF DOCUMENT | ZM-SEC-001 v1.0.0