Security & Infrastructure Transparency Policy

Last Updated: 14 March 2026

Company Registration Number: 17091516
ICO Registration: Pending

1. Purpose

This Security & Infrastructure Transparency Policy explains how **Zentrix Hosting Ltd** ("Zentrix Hosting", "we", "us", or "our") manages the security, reliability, and integrity of the infrastructure used to provide our hosting services.

The goal of this policy is to provide transparency regarding the security practices used to protect:

- customer infrastructure
- hosted data
- network operations
- the broader internet ecosystem

This document complements our **Privacy Policy, Data Processing Agreement, and GDPR Compliance Policy**.

2. Infrastructure Overview

Zentrix Hosting operates and manages infrastructure used to provide services including:

- web hosting
- VPS hosting
- game server hosting
- bot hosting

managed hosting services

Infrastructure components may include:

virtualization platforms
storage systems
network equipment
management systems
monitoring and logging systems

Infrastructure may be operated directly by Zentrix Hosting or through trusted datacenter partners.

3. Physical Security

Datacenter facilities used by Zentrix Hosting implement physical security measures such as:

controlled facility access
CCTV surveillance
access logging
environmental monitoring
fire suppression systems
redundant power systems

Access to physical infrastructure is restricted to authorized personnel only.

4. Network Security

Zentrix Hosting maintains security measures designed to protect network infrastructure.

These measures may include:

enterprise-grade firewalls
network segmentation
traffic filtering

DDoS mitigation strategies
monitoring for malicious traffic
automated intrusion detection systems

Network traffic may be analyzed for the purpose of identifying abuse, attacks, or infrastructure threats.

5. Infrastructure Security

Systems used to operate Zentrix Hosting infrastructure are secured through multiple layers of protection.

Security practices include:

secure virtualization environments
operating system hardening
regular security patching
vulnerability monitoring
restricted administrative access
secure authentication methods

Administrative access to infrastructure is limited to authorized personnel.

6. Access Controls

Zentrix Hosting uses strict access control policies.

These include:

role-based access permissions
least-privilege access principles
authentication logging
restricted administrative access

Access rights are reviewed periodically to ensure they remain appropriate.

7. Monitoring and Logging

Infrastructure is monitored continuously to maintain reliability and security.

Monitoring systems track:

- network activity
- infrastructure health
- system performance
- security events

Logs may be retained for security investigation, troubleshooting, and compliance purposes in accordance with our **Data Retention Policy**.

8. Vulnerability Management

Zentrix Hosting regularly reviews systems for potential security vulnerabilities.

Security management practices include:

- applying operating system updates
- patching critical security issues
- monitoring vendor security advisories
- investigating potential infrastructure risks

Where necessary, security fixes may be applied immediately to protect infrastructure.

9. Incident Response

Zentrix Hosting maintains procedures for responding to security incidents.

These procedures include:

identifying and isolating affected systems
investigating the source of the incident
mitigating the impact of the incident
restoring normal service operations

Where appropriate, customers may be notified of incidents affecting their services.

10. Abuse and Security Reporting

Security researchers and members of the public may report security vulnerabilities or abuse incidents.

Reports can be submitted to:

Security Contact:
security@zentrixhosting.com

Abuse Contact:
abuse@zentrixhosting.com

We encourage responsible disclosure of vulnerabilities.

11. Customer Security Responsibilities

Customers using Zentrix Hosting services are responsible for maintaining the security of their hosted systems.

Customers should:

keep operating systems updated
secure administrative access
monitor applications for vulnerabilities
maintain secure authentication practices

Zentrix Hosting is not responsible for vulnerabilities within customer-managed applications or software.

12. Transparency and Trust

Zentrix Hosting is committed to maintaining transparency regarding infrastructure operations and security practices.

While we strive to provide useful information, certain security details may be withheld where disclosure could increase the risk of infrastructure attacks.

13. Policy Updates

This policy may be updated periodically to reflect changes in infrastructure practices, security standards, or regulatory requirements.

The most recent version will always be published on our website.

Contact Information

Zentrix Hosting Ltd

3rd Floor
86–90 Paul Street
London
England
United Kingdom
EC2A 4NE

Security Contact:
security@zentrixhosting.com

General Contact:
contact@zentrixhosting.com

Authorised by

Alex Cheetham
Chief Executive Officer
Zentrix Hosting Ltd