Waypoint Platform Group: security audit report

Created on 13 August 2026 @ 22:34

Waypoint Platform Group wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at Waypoint Platform Group is being monitored and safeguarded from the developer's computer all the way to the infrastructure used for delivery.

This security report has been generated by Aikido Security based on real-time monitoring of Waypoint Platform Group code and infrastructure.

ISO 27001:2022 compliance

A brief overview of the ISO 27001 requirements and any measures taken for these.

Title	Taken measures
A.8.2 - Privileged access rights	✓ Has checks in place for enforcing permissions
A.8.3 - Information access restriction	✓ Prevents public access to cloud resources ✓ Has proper access controls for cloud resources
A.8.5 - Secure authentication	✓ Requires MFA for cloud users ✓ Enforces encryption of data in transit
A.8.6 - Capacity management	✓ Has budgeting alerts set up ✓ Uses load balancers correctly
A.8.7 - Protection against malware	✓ Prevents unwanted write operations to filesystems ✓ Has enabled threat detection ✓ Uses Lockfiles to pin code dependencies
A.8.8 - Management of technical vulnerabilities	✓ Does not have any issues outside of their SLA
A.8.12 - Data leakage prevention	✓ Securely stores files ✓ Prevents remote code execution ✓ Is protected against SSRF attacks ✓ Has measures against SQL injection attacks ✓ Prevents XSS attacks
A.8.13 - Backups	✓ Has backups for stateful cloud resources ✓ Has cross account backups enabled
A.8.15 - Logging	✓ Enabled security logging for cloud instances

A.8.18 - Use of privileged utility programs	✓ Enforces secure access for cloud users ✓ Prevents the exposure of sensitive data ✓ Requires MFA for cloud users ✓ Has proper access controls for cloud resources
A.8.20 - Network security	✓ Prevents unauthorized network access
A.8.31 - Separation of development, test and production environments	Monitoring, not fully compliant
A.8.24 - Use of cryptography	✓ Enforces safe SSL protocol usage ✓ Uses secure cookies ✓ Uses up-to-date cryptographic libraries
A.8.9 - Configuration management	✓ Runs cloud instances on up-to-date versions ✓ Uses Lockfiles to pin code dependencies
A.8.16 - Monitoring activities	✓ Has connected a cloud environment ✓ Receives security alerts in real time ✓ Has enabled threat detection
A.8.25 - Secure development lifecycle	✓ Uses a CI integration ✓ Has connected a code repository ✓ Has connected a cloud environment
A.8.28 - Secure coding	✓ Does not have any issues outside of their SLA
A.8.32 - Change management	✓ Tracks progress via an issue tracker
A.5.15 - Access control	✓ Applies the least privilege principle for cloud users ✓ Applies the least privilege principle for cloud resource ✓ Applies the least privilege principle to cloud resources ✓ Prevents the exposure of sensitive data
A.5.16 - Identity management	✓ Properly manages the identity of cloud users

A.5.28 - Collection of evidence	✓ Has budgeting alerts set up ✓ Enabled security logging for cloud instances ✓ Has enabled threat detection
A.5.33 - Protection of records	✓ Prevents public access to cloud resources ✓ Encrypts data at rest