NexWave Security & Infrastructure Overview

How NexWave protects business data across hosting infrastructure, application-layer controls, tenant configuration, encryption, auditability, incident response, and scoped security review.

Version 1.2 · June 2026

nexwaveapp.com/security/ · security@nexwaveapp.com

Security model

NexWave is delivered as a managed SaaS product to small and mid-sized businesses across New Zealand, Australia and the United Kingdom. Security responsibilities are clearest when each layer is described separately.

Hosting provider layer

AWS-backed managed infrastructure, regional hosting options, monitoring, backup operations, incident response coordination, and provider SOC 2 Type II, ISO 27001:2022 and ISO 9001:2015 certifications.

NexWave application layer

NexWave-specific code, integrations, implementation changes, application controls, security scanning, dependency checks, and issue triage.

Customer tenant policy

User onboarding, role assignment, identity settings, session policy, third-party integrations, data classification, and internal access governance.

> **Certification scope:** The hosting provider maintains SOC 2 Type II, ISO 27001:2022 and ISO 9001:2015 certifications for the relevant cloud and operating environment. NexWave does not currently hold separate SOC 2, ISO 27001 or ISO 9001 certification for NexWave-specific application code, integrations or customer-specific customisations.

Why this distinction matters

Cloud and hosting certifications are valuable, but they do not automatically certify all product-specific code and customisations above that layer. NexWave therefore separates hosting-provider certifications from NexWave application-layer security practices.

Hosting-provider certifications

NexWave customer instances run on AWS-backed managed hosting infrastructure. The hosting provider maintains SOC 2 Type II, ISO 27001:2022 and ISO 9001:2015 certifications for the relevant cloud and operating environment.

Certification	Layer	Scope note
Provider SOC 2 Type II	Hosting and cloud operating environment	Applies to the provider's audited hosting or cloud operating environment, subject to the scope of the provider certification.
Provider ISO 27001:2022	Hosting and information security controls	Applies to the provider's information security controls, subject to the scope of the provider certification.
Provider ISO 9001:2015	Hosting and quality management controls	Applies to the provider's quality management controls, subject to the scope of the provider certification.
Data protection alignment	NexWave and customer tenant configuration	NexWave supports data subject access, export and deletion workflows where required by applicable privacy obligations. This is not a certification.

NexWave certification position

NexWave does not currently hold separate SOC 2, ISO 27001 or ISO 9001 certification for the NexWave product company, NexWave-specific application-layer code, integrations or customer-specific customisations. NexWave's own work focuses on secure application development, security scanning, release controls and customer-configured tenant controls.

NexWave application-layer security practices

NexWave-specific code and implementation changes are reviewed, tested and scanned through the standard release workflow before they reach customers.

Peer review

Product changes use feature branches and pull requests. Security-sensitive changes receive engineering review before release.

Automated testing

Automated tests run in CI for supported repositories. Higher-risk customer-facing workflows receive manual QA in addition to developer testing.

Static analysis

Semgrep is used to scan application code for security-sensitive patterns, correctness issues and framework-specific risks.

Dependency scanning

GitHub Dependabot, pip-audit and OSV-Scanner are used to identify vulnerable third-party packages and open-source dependency risk.

Secret and configuration scanning

Trivy scanning supports vulnerability, secret, misconfiguration and licence checks as part of the security reporting workflow.

Report artefacts

Reports can include JSON, SARIF, text, Markdown and HTML artefacts. Findings are triaged and tracked for remediation.

Security patching

Security advisories and dependency alerts are reviewed through the engineering workflow and released according to severity, exposure and customer change windows.

Scoped customer testing

Customer-specific penetration testing and application-layer review can be scoped with written agreement on target, timing and methodology.

Scanner outputs, suppression notes and detailed workflow artefacts are shared only with qualified prospects or customers under an agreed process.

Infrastructure, isolation & encryption

Hosting and data residency

NexWave runs on AWS-backed managed infrastructure. Customer tenants can be pinned to a chosen AWS region at provisioning, including **Sydney (ap-southeast-2)** for ANZ data residency.

Tenant isolation

On the standard tier, each customer tenant is logically isolated with separate database, file storage, user pool, credentials and session context. For customers that require stronger isolation than logical tenancy, NexWave can scope dedicated infrastructure or a bring-your-own-server model.

Layer	Implementation
In transit	TLS 1.2 or higher on customer endpoints. Administrative server access uses key-based or certificate-based SSH rather than passwords.
Application secrets	User passwords are hashed. API keys, OAuth tokens and third-party connector credentials are stored encrypted and decrypted only at point of use.
Storage layer options	Dedicated and bring-your-own-server tiers can be configured with AWS-native at-rest encryption and customer-managed keys where required.
Backups	Offsite backups are taken daily with multi-tier retention. Backup encryption can be enabled where a customer's security policy requires it.

Application security controls

NexWave provides practical controls for access, identity, session policy, auditability and integration governance. Tenant administrators configure them to match their organisation's policy.

Role-based access control

Permissions at the role, document and field level. Users see only the records and fields their role grants them.

Two-factor authentication

2FA and one-time password support are available and can be enforced for privileged roles.

Single sign-on

OAuth 2.0, OpenID Connect and LDAP support are available for common identity-provider setups.

IP restrictions

Per-user IP allow-listing can restrict administrative accounts to your corporate network or VPN.

Password and session policy

Tenant administrators can configure password strength, expiry, session timeout and idle expiry policies.

Audit trail

Activity logs, route history, document timeline and version tracking support investigation and change review.

API and integration governance

Integration credentials are stored encrypted. Customer-specific endpoints are reviewed for authentication, permission and rate-limiting requirements.

Support access

Support access is granted in the customer context and can be limited, reviewed and logged through tenant controls.

Incident response & shared responsibility

Incident response

Security issues are triaged by severity and handled through the engineering and support workflow. For hosting-layer incidents, NexWave coordinates with the relevant infrastructure response teams and communicates with affected customers.

Customer notification process

In the event of a confirmed incident affecting customer data, NexWave notifies affected customers through nominated security contacts as soon as practical, with the information available at that point. A written post-incident report can be provided once the investigation is closed. Any specific notification timeline is governed by the applicable agreement.

Security response targets

Contractual response targets can be agreed for customers with specific security requirements, including CVSS-based severity bands where appropriate. Where agreed, those targets are documented in the relevant agreement.

Vulnerability disclosure

NexWave International maintains a published Vulnerability Disclosure Policy at **https://nexwaveapp.com/security/**. Vulnerability reports should be sent to **security@nexwaveapp.com**. This mailbox is for security reports and is not a 24/7 emergency hotline.

The policy covers authorised NexWave-specific vulnerability reports, permitted testing, out-of-scope testing, prohibited activity, confidentiality and coordinated disclosure. NexWave does not operate a public bug bounty programme unless separately agreed in writing.

Where a validated NexWave-specific vulnerability requires coordinated public disclosure, NexWave International will request CVE assignment through MITRE's CNA of Last Resort or another appropriate CVE Numbering Authority.

Shared responsibility

What NexWave provides

Hosted on provider infrastructure with SOC 2, ISO 27001 and ISO 9001 certifications. Logical or single-tenant hosting options. Application-layer review, testing and scanning practices. RBAC, 2FA, SSO, IP restrictions, password policy and audit trail controls. Backup, incident response and customer notification processes.

What you configure

User onboarding, offboarding and role assignment. 2FA, SSO, password and session policies. IP restrictions for privileged accounts. Third-party integrations and credentials. Internal data classification and access governance.

As part of onboarding, the NexWave team can work through a security configuration checklist with your nominated security contact and document the baseline applied to your tenant.

Common security questions

Does NexWave hold SOC 2 or ISO 27001 certification?

The hosting provider maintains SOC 2 Type II, ISO 27001:2022 and ISO 9001:2015 certifications for the relevant cloud and operating environment. NexWave does not currently hold separate SOC 2, ISO 27001 or ISO 9001 certification for NexWave-specific application code, integrations or customer-specific customisations.

What certification or testing coverage applies?

SOC 2, ISO 27001 and ISO 9001 apply at the hosting-provider layer. Customer-specific application-layer penetration testing can be scoped separately against your tenant with written agreement on timing, target and methodology.

How is NexWave-specific code reviewed?

NexWave-specific changes are reviewed, tested and scanned through the standard release workflow. The security reporting workflow includes Semgrep, Trivy, pip-audit and OSV-Scanner outputs that can be packaged for qualified reviews where appropriate.

Where is my data hosted?

NexWave runs on AWS-backed managed infrastructure. Your tenant is pinned to a chosen AWS region at provisioning, including Sydney (ap-southeast-2) for most ANZ customers.

Who can access my data inside NexWave?

Only users your administrators create and assign roles to. Access by NexWave support staff requires customer approval for the support context and is logged in the tenant audit trail.

Can we run our own penetration test?

Customer-initiated testing requires advance written agreement on scope, methodology and timing. NexWave can also help scope targeted application-layer testing.

How do I report a vulnerability?

Email security@nexwaveapp.com with the affected URL or product area, reproduction steps, impact, safe evidence and your contact details. The published Vulnerability Disclosure Policy is available at https://nexwaveapp.com/security/.

Do you define security response targets?

Security findings are triaged by severity. Contractual response targets can be agreed for customers with specific security requirements.

What happens to my data if we leave?

On termination, tenant data is exported in machine-readable form and made available for an agreed period, then securely deleted under the relevant agreement and retention policy.

Contact

Questions about this overview, security questionnaires, or specific compliance requirements?

Security reports: security@nexwaveapp.com
General enquiries: support@nexwaveapp.com
Web: https://nexwaveapp.com/security/
Security.txt: https://nexwaveapp.com/.well-known/security.txt
Contact form: https://nexwaveapp.com/contact/

This document is provided for informational purposes only and may be updated without notice. Specific contractual commitments are governed by the NexWave SaaS Subscription Agreement and any executed Data Processing Addendum. Document version 1.2, June 2026.