NexWave Security & Compliance Overview

How NexWave protects your business data, end to end. Architecture, certifications, development practices, encryption, application controls, audit trail, and incident response, in one document for your security review.

Version 1.0 · May 2026

nexwaveapp.com · support@nexwaveapp.com

Platform architecture

NexWave is delivered as a managed SaaS product to small and mid-sized businesses across New Zealand, Australia and the United Kingdom. The platform is composed of three layers, each with its own clearly-scoped security controls and accountability.

1. NexWave application

NexWave is developed and operated by NexWave International. NexWave is built on top of **ERPNext**, the leading fully open-source ERP application, and the **Frappe Framework** that underpins it. On top of the open-source core, NexWave adds regional localisations (NZ GST, AU BAS reporting, AS/NZS compliance hooks, payroll and other ANZ-specific modules) and customer-specific extensions for individual implementations.

2. Open-source core (ERPNext, Frappe Framework)

ERPNext and the Frappe Framework are developed and maintained by **Frappe Technologies Private Limited**. They are fully open source under the GNU GPL v3 licence. The codebase is publicly available on GitHub (34,000+ stars and 11,000+ forks on ERPNext alone) and is continuously reviewed and contributed to by an external developer community worldwide. Vulnerabilities are reported through a public security-advisory process and patched in the open. NexWave tracks upstream advisories and updates customer instances to the latest patch versions on Frappe's cadence.

3. Cloud hosting (Frappe Cloud on AWS)

NexWave customer instances are hosted on **Frappe Cloud**, the managed cloud platform operated by Frappe Technologies. Frappe Cloud runs on Amazon Web Services and offers 13 regional locations, including **Sydney (ap-southeast-2)** which is the default for ANZ customers. Customer tenants can be pinned to a specific region at provisioning. Frappe Cloud is the cloud-hosting layer in NexWave's stack and the party whose third-party certifications (SOC 2 Type II, ISO 27001, ISO 9001) apply to the infrastructure NexWave runs on.

Why this matters for your security review

Two of NexWave's three layers (the open-source core and the hosting platform) sit with Frappe Technologies. Frappe holds the independent security certifications that cover those layers. NexWave does not duplicate certifications already held by the layers it builds on; it adds customer-specific configuration, localisation and extensions on top, following the framework's existing security primitives rather than introducing parallel control planes.

Compliance & certifications

The certifications below are held by Frappe Technologies (the developer of ERPNext, the Frappe Framework, and Frappe Cloud) and apply to the layers NexWave is built on and runs on. Reports and certificates can be shared with qualified prospects and customers on request through your NexWave account team.

Standard	Status	Scope & details
SOC 2 Type II	1 Jun 2024 – 31 May 2025 audit window	Covers the Security, Availability and Confidentiality Trust Services Criteria for Frappe Cloud, the hosting service NexWave runs on. Independent third-party attestation.
ISO 27001:2022	Certified, surveillance audit Dec 2025	Certifying body: ISOQAR. Information Security Management System covering Frappe's engineering, customer support and partnership functions (on-premises and SaaS), within which both the Frappe Framework and ERPNext are developed. Upgraded from ISO 27001:2013 in December 2024.
ISO 9001:2015	Certified, surveillance audit Dec 2025	Certifying body: ISOQAR. Quality Management System. Supporting evidence of a documented management system, continuous improvement processes, and customer-satisfaction practices.
GDPR	Compliant	Data-handling practices aligned with the EU General Data Protection Regulation, including data subject access, deletion and portability rights.

NexWave's own certifications

NexWave does not hold a separate SOC 2 attestation for itself. NexWave is a software product based on ERPNext (covered by Frappe's ISO 27001 ISMS) and runs on Frappe Cloud's SOC 2 Type II certified infrastructure. The certifications sit at the layer where the controls are actually operated. For customers requiring an independent NexWave-specific attestation, a roadmap discussion is available through your account team.

Penetration testing

Frappe Cloud completes periodic third-party penetration testing (VAPT) of the platform and framework, in addition to regular internal and external vulnerability scans. The most recent VAPT executive summary, including the test date and confirmation of remediation status for any High or Critical findings, can be facilitated on request through the same channel as the SOC 2 report.

For customers who want assurance over their specific tenant, including any custom code or integrations in scope, a targeted application-layer penetration test can be scoped using industry-standard tooling aligned to OWASP testing methodology (e.g. OWASP ZAP, Burp Suite), and the executive summary shared with the customer.

Secure development lifecycle

Security is enforced at every stage of NexWave's build pipeline, not added at the end before release. The same controls apply to the underlying Frappe Framework and ERPNext, which are developed inside Frappe's ISO 27001 certified ISMS.

Source control & peer review

Git with feature branches. Every change is reviewed by a second engineer before merge. No solo merges to release branches.

AI-assisted security review

Every pull request runs through an AI reviewer that surfaces injection risks, unsafe deserialisation, secret leakage and broken access checks before the human reviewer sees them.

Static analysis (SAST)

Semgrep runs in CI on every pull request, using the Frappe security ruleset and Semgrep's `python.lang.correctness` ruleset. Findings are triaged before merge.

Dependency scanning

GitHub Dependabot continuously alerts on vulnerable third-party packages across every repository. **pip-audit** runs in CI to check Python dependencies on every pull request.

CI test gating

Unit and integration tests run on every pull request. Changes do not merge until all automated tests pass. No exceptions.

Manual QA

Higher-risk changes go through a dedicated QA pass in addition to developer testing, exercising the same flows a customer would.

Framework patching

Upstream Frappe and ERPNext security advisories are tracked through the public GitHub Security Advisories channel. Patches are deployed to customer instances on the upstream cadence.

Custom code follows framework primitives

Customer-specific customisations reuse the framework's authentication, permission and rate-limiting controls. We do not roll our own auth or permission models.

DAST: NexWave does not currently run automated dynamic-analysis tooling in the standard CI pipeline. OWASP ZAP baseline scans against a staging instance can be scoped for customers who require them.

Infrastructure, isolation & encryption

Hosting

NexWave runs on Frappe Cloud, which is deployed on Amazon Web Services. Customer tenants can be pinned to a specific AWS region at provisioning, including **Sydney (ap-southeast-2)** for ANZ data residency. 12 other regions are available globally.

Multi-tenant isolation (standard tier)

On the standard tier, each customer is a logically isolated tenant: separate database, separate file store, separate Redis namespace, separate user pool and credentials. There is no cross-tenant data access path by design. This is consistent with how mainstream SaaS platforms (Xero, Salesforce, Atlassian, Notion) deliver multi-tenant services with logical isolation.

Stricter isolation tiers

For customers whose security policy requires stronger isolation than logical separation, Frappe Cloud offers two upgrades:

- **Dedicated server tier**: the customer's NexWave instance runs on its own AWS EC2 instance, not shared with any other customer. Equivalent at-rest encryption settings (EBS, RDS) can be confirmed and configured at provisioning.
- **Bring-Your-Own-Server (BYOS)**: the NexWave instance is deployed inside the customer's own AWS account, with full customer control over the underlying infrastructure, including KMS-managed encryption keys, VPC peering, logging and billing.

Encryption

Layer	Implementation
In transit	TLS 1.2+ on all customer endpoints. Server-side SSH access uses certificate or public-key authentication only; passwords are not accepted.
Application secrets at rest	User passwords hashed with modern algorithms. API keys, OAuth tokens and third-party connector credentials are stored encrypted via the framework's `Password` field type. Never returned through APIs; decrypted only at point of use.
Database at rest (dedicated/BYOS)	AWS-native EBS and RDS encryption with KMS-managed keys configurable at provisioning. Customer-managed keys supported on BYOS.
Backups	Daily offsite backups with multi-tier retention (7 daily, 4 weekly, 12 monthly, 10 yearly). Backup encryption (fernet, AES + HMAC) is configurable and enabled for customers whose security policy requires it.

Application security controls

The Frappe Framework provides a set of security primitives that ship out of the box with every NexWave deployment. 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 OTP support built in. Enforceable at the role level, including required-for-privileged-roles policies.

IP-based access restriction

Per-user IP allow-listing for restricting administrative accounts to your corporate network or VPN.

Password policies

Configurable minimum length, complexity, history and expiry. Passwords hashed with modern algorithms.

Session management

Configurable session timeout and idle expiry. Active sessions can be viewed and revoked per user.

API rate limiting

Uniform rate limits across all platform endpoints, including customer-specific endpoints added during implementation.

Single sign-on (SSO)

OAuth 2.0 / OpenID Connect and LDAP. Integrations available for Microsoft Entra ID, Google Workspace and others.

Audit trail

Route history, activity log, document timeline, and document version tracking. Full reconstruction of who did what and when.

Audit & forensic trail

Every meaningful action in NexWave is recorded with the user, the change and the timestamp. Investigation, dispute resolution and forensic reconstruction work on real data, not best guesses.

- **Activity log** records significant user actions (logins, document operations, key configuration changes) with user, timestamp and outcome.
- **Route history** captures navigation events per user.
- **Document timeline** records every change to business-critical records (sales orders, invoices, stock movements, payments) with the user who made it and when.
- **Document version tracking** retains prior versions of records, supporting reconstruction of the full change history.

Incident response & data residency

Data residency

Customer tenants are pinned to a chosen AWS region at provisioning. Most ANZ customers run in **Sydney (ap-southeast-2)**. Backup encryption (fernet, AES + HMAC) is configurable on Frappe Cloud and is enabled at provisioning for customers whose data-protection policy requires it.

Incident response programme

Frappe Cloud operates an incident response programme as part of its ISO 27001 and SOC 2 controls, with detection, triage, containment, customer notification and post-incident review documented and audited. NexWave coordinates with Frappe Cloud's response team for any incident affecting the underlying platform.

Breach notification commitment

In the event of a confirmed breach affecting customer data, NexWave will notify the nominated security contacts **without undue delay, and in any event within 72 hours of becoming aware**, with the information available at that point. A written post-incident report follows once the investigation is closed, covering what happened, impact assessment, remediation and corrective actions.

Shared responsibility

Security in practice is a joint effort. NexWave ships the platform with strong defaults and a comprehensive set of controls. Tenant administrators configure them to match your organisation's risk tolerance.

What NexWave provides

Certified cloud infrastructure with logical or single-tenant isolation. Encryption in transit and for application-layer secrets. RBAC, 2FA, IP restrictions, password policies, audit trail as platform primitives. Daily offsite backups with configurable encryption. Vulnerability monitoring, patching cadence and SAST in CI. Incident response and 72-hour breach notification.

What you configure

2FA enforcement policy across user roles. Password policy strength, expiry and history. Session timeout and IP restrictions on privileged accounts. User onboarding, offboarding and role assignment. Third-party integrations enabled and the credentials used. Internal data classification and access governance.

As part of onboarding, our team works through a security configuration checklist with your nominated security contact and documents the baseline applied to your tenant.

Common security questions

Where is my data hosted?

NexWave runs on AWS via Frappe Cloud. Your tenant is pinned to a chosen AWS region at provisioning, including Sydney (ap-southeast-2) for ANZ customers.

Who can access my data inside NexWave?

Only users your administrators have created and assigned roles to. Access by NexWave support staff requires explicit invitation from the customer for the duration of a support ticket and is logged in the tenant audit trail.

Can I get a copy of the SOC 2 Type II report?

Yes. Frappe Cloud's SOC 2 Type II report, ISO 27001:2022 certificate and ISO 9001:2015 certificate can be facilitated on request through your NexWave account team. Some artifacts require an NDA, which Frappe Cloud handles directly.

Do you support SSO?

Yes. OAuth 2.0 / OpenID Connect and LDAP, with integrations for Microsoft Entra ID, Google Workspace and other common identity providers.

Can we run our own penetration test against our tenant?

Customer-initiated testing requires advance written agreement on scope, methodology and timing. NexWave can also scope a targeted application-layer penetration test using industry-standard tooling aligned to OWASP methodology, and share the executive summary.

What happens to my data if we leave?

On contract termination, tenant data is exported in machine-readable form (CSV and database backup) and made available to you for a defined period, after which it is securely deleted in line with our data retention policy.

How are subprocessors managed?

A current list of subprocessors is maintained and shared on request. Material changes are notified to customers in advance.

Contact

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

Email: support@nexwaveapp.com
Web: https://nexwaveapp.com/security/
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 Master Services Agreement and any executed Data Processing Addendum. Document version 1.0, May 2026.