SYNTAQ

Information Security & Data Protection

Data Storage & IT Security Whitepaper

How Syntaq stores, secures, and safeguards client data across its hosted platforms

Field	Detail
Document	Data Storage & IT Security Whitepaper
Prepared by	Syntaq
Version	1.0
Issue date	10 June 2026
Classification	Public — approved for client distribution
Certification	ISO/IEC 27001:2022, certified (certificate available on request)
Regulatory alignment	Australian Privacy Act 1988 (Cth) & Australian Privacy Principles; NZ Privacy Act 2020

This document is provided to assist clients in satisfying their due-diligence and regulatory obligations, including the security requirements of the Office of the Australian Information Commissioner (OAIC) under Australian Privacy Principle 11. It describes the security protocols Syntaq applies and the specific steps taken to safeguard client data.

Contents

1. Overview

Security and data security in particular is at the forefront of Syntaq's design and operating principles. We understand that the data we hold and process on behalf of our clients and their customers is sensitive, valuable, and frequently subject to regulatory protection. This whitepaper sets out, in practical detail, how that data is stored, how it is protected in transit and at rest, who can access it, and how we maintain and assure those controls over time.

Syntaq operates an Information Security Management System (ISMS) that has been independently certified to ISO/IEC 27001:2022. Our ISMS is supported by a full suite of approved, version-controlled security policies — covering access control, cryptography, information handling, secure development, backup and recovery, incident management, supplier management, and business continuity each reviewed at least annually.

Importantly, Syntaq delivers applications across two distinct, separately-governed hosting environments. The controls differ in implementation between them, and this document describes each environment clearly so that you can match the information to the specific application you use.

1.1 Our security posture at a glance

Area	Position
Certification	ISO/IEC 27001:2022 certified ISMS
Encryption in transit	TLS 1.2 minimum enforced on all client-facing endpoints
Encryption at rest	AES-256 across databases, file storage, and backups
Authentication	Multi-factor authentication (MFA) on all administrative and deployment access; application-level authentication for end users
Access model	Role-based access control on a least-privilege basis; quarterly access reviews
Backups	Automated backups with point-in-time restore; restorations tested on a defined schedule
Monitoring	Continuous platform monitoring, dependency vulnerability scanning, and secret scanning
Breach response	Documented incident management aligned to the Notifiable Data Breaches (NDB) scheme

2. Regulatory alignment with OAIC and the Australian Privacy Principles

Syntaq is an Australian company and handles personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). Where clients have New Zealand operations, our controls are also aligned with the NZ Privacy Act 2020.

Australian Privacy Principle 11 (Security of personal information) requires an entity to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. The controls

described in this whitepaper are the reasonable steps Syntaq takes to meet that obligation. In summary:

OAIC / APP focus	How Syntaq addresses it
Protect from unauthorised access	MFA, role-based least-privilege access, Row Level Security on multi-tenant data, and quarterly access reviews
Protect from loss	Encrypted, automated backups with tested point-in-time restore, and documented disaster-recovery objectives
Protect from misuse / interference	Encryption in transit and at rest, secure development lifecycle, dependency and secret scanning, and continuous monitoring
Destruction / de-identification	Defined data-retention schedule with secure deletion on contract termination
Notifiable Data Breaches scheme	Documented incident-management process with assessment, containment, and notification to the OAIC and affected individuals where a breach is likely to result in serious harm
Transparency	Published Privacy Policy; data-processing terms set out in customer agreements

Syntaq maintains a Legal and Regulatory Register that tracks these obligations and confirms compliance status, and these obligations are reviewed as part of our ISMS management-review cycle.

3. Two hosting environments, which applies to you

Syntaq applications are delivered through one of two environments. The security objectives — confidentiality, integrity and availability of your data — are identical in both; the underlying technology and the specific controls differ. The table below summarises the distinction; the following sections describe each in detail.

Dimension	Managed Service Environment	Azure-Hosted Platforms
Typical applications	Purpose-built / managed-service applications (e.g. document-structuring and workflow apps)	Syntaq Falcon and the SBOS Portal
Compute / hosting	Vercel (serverless / edge hosting)	Microsoft Azure (App Service)
Data store	Supabase (managed PostgreSQL) with Row Level Security	Azure SQL Database
File storage	Managed object storage within the project	Azure Blob Storage
Source control	GitHub (private)	GitHub (private)
Secrets	Vercel encrypted environment variables (server-side only)	Azure Key Vault
Region	Provisioned per project; specific region confirmed on request	Australia East

4. Managed Service Environment (Supabase + Vercel)

This environment hosts purpose-built applications on Vercel for compute and edge delivery, with Supabase (managed PostgreSQL) for data storage and authentication, and GitHub for private source control. Each of these is an established, independently-audited platform provider, and Syntaq layers its own ISO 27001 controls on top.

4.1 Data storage and tenancy

- Client data is stored in a managed Supabase PostgreSQL database. Data created or stored in the application is classified as Confidential (at minimum) under Syntaq's information classification scheme and handled accordingly.
- Where data is multi-tenant or stored on a per-customer basis, Row Level Security (RLS) policies are enforced at the database level so that records are only accessible to the authorised tenant. RLS is mandatory for shared-credential, multi-tenant tables.
- File and object data is held in managed storage within the project, subject to the same access and encryption controls.
- Production data is never copied to local developer machines for testing; development environments use isolated test data, not the live database.

4.2 Encryption

Layer	Protection
In transit	TLS 1.2 minimum on all connections between users, the application, and the database
At rest — database	AES-256 encryption applied by the managed database platform
At rest — file storage	AES-256 encryption applied by the managed storage platform
Secrets / credentials	Held only in Vercel server-side encrypted environment variables — never in client bundles, never committed to source control

4.3 Access control and authentication

- Multi-factor authentication (MFA) is enforced on every account that can administer or deploy the application (GitHub and Vercel). There are no shared administrator credentials.
- Repositories are private. Access to the hosting, database, and source-control platforms is granted on a least-privilege basis and reviewed at least annually, with stale access removed promptly.
- End-user authentication within the application is handled through the platform's authentication providers (Supabase Auth), with the privileged service credential restricted to server-side use only.

4.4 Secure development and change management

- The production branch is branch-protected: no direct changes are permitted. Every change to production reaches it through a reviewed, merged pull request, creating an immutable, timestamped change record.
- Deployments are automated from source control, with preview deployments for work prior to release. Even emergency changes follow the pull-request path so the audit trail remains complete.

- Development follows Syntaq's Secure Development policy and incorporates the OWASP Top 10 as a baseline. Security requirements (authentication, authorisation, server-side input validation, safe data handling) are reviewed for each significant feature before release.
- GitHub Dependabot (dependency vulnerability alerts) and secret scanning run continuously across the repository. High and critical findings are remediated or formally risk-accepted with an owner and date.

4.5 Backups, recovery and continuity

- Production data is backed up using a managed database plan that supports backups and point-in-time recovery. Backup restoration is tested to a non-production target at least annually, with the result logged, confirming backups are not merely configured but genuinely recoverable.
- The application can be redeployed from source control to restore service. Recovery objectives are measured in hours: the application is recovered from GitHub via Vercel, and the database from the most recent Supabase backup or point-in-time recovery point.

4.6 Logging, monitoring and vulnerability management

- Vercel request and deployment logs and Supabase database and authentication logs are retained and available to investigate access or abuse.
- Technical vulnerabilities are reviewed quarterly through Dependabot, with remediation, risk acceptance, or deferral recorded for each review.
- Any additional service that receives or processes client data (for example email delivery, analytics, or payment processing) is recorded and kept current as part of our supplier and data-flow management.

5. Azure-Hosted Platforms (Syntaq Falcon & SBOS Portal)

Syntaq's Falcon platform and SBOS Portal are hosted, maintained and delivered on Microsoft Azure cloud services in the Australia East region. These platforms benefit from Azure's enterprise-grade infrastructure together with Syntaq's own ISO 27001 controls.

5.1 Data storage and encryption

Data type	Storage & encryption
Databases (at rest)	Azure SQL with Transparent Data Encryption (TDE) - AES-256
File storage (at rest)	Azure Blob Storage Service Encryption (SSE) - AES-256
Data in transit	TLS 1.2 minimum, enforced at the edge via Azure Front Door
Application secrets	Azure Key Vault (AES-256), access restricted via Azure RBAC and MFA
Backups	Encrypted by the platform - AES-256

5.2 Access, authentication and key management

- Access is governed by Azure role-based access control (RBAC) on a least-privilege basis, with multi-factor authentication required for administrative and privileged access.

- Cryptographic keys are managed in Azure Key Vault, rotated at least annually or on suspected compromise, with access logs reviewed quarterly. Keys are never stored in source code or configuration.
- Public TLS certificates are issued and renewed automatically, with expiry monitored so certificates never lapse in production.

5.3 Availability, backups and disaster recovery

- Syntaq operates hosted disaster-recovery services provided by Microsoft Azure for application servers, database servers, and user files (forms and document templates).
- A point-in-time restore facility allows recovery of a historical version of the database from within the retention window (short-term automated backups plus long-term retention), enabling recovery from corruption or accidental change.
- Backups are geo-redundant across Azure paired regions, and restorability is verified through quarterly test restores and an annual full disaster-recovery test.

5.4 Monitoring and secure development

- Microsoft Defender for Cloud and Defender for Endpoint provide continuous threat monitoring across Azure and managed endpoints.
- Development follows the same Secure Development lifecycle and OWASP Top 10 baseline described above, with Dependabot and secret scanning on all repositories and changes promoted through reviewed pull requests.

6. Controls that apply across both environments

6.1 Data classification and handling

Syntaq applies a four-tier classification scheme - Public, Internal, Confidential, and Highly Confidential, aligned to Microsoft 365 sensitivity labels. Data processed on behalf of clients is classified as Confidential by default; raw exports or datasets containing personal information at scale are treated as Highly Confidential. Each level carries defined handling, encryption, transfer, and storage requirements, and approved versus prohibited channels for moving information are documented and auditable.

6.2 Cryptography standards

Encryption is governed by an approved Cryptography and Key Management Policy. Approved standards include AES-256 for data at rest and TLS 1.2 minimum for data in transit. Weak or homebrew cryptography (for example MD5 or SHA-1 for security purposes, self-signed certificates in production, or under-strength keys) is prohibited.

6.3 Threat intelligence

Syntaq is registered with the Australian Cyber Security Centre (ACSC) advisory service and consumes continuous threat intelligence from Microsoft Defender, GitHub Dependabot, and vendor security advisories. Advisories are triaged through our change, vulnerability, and incident processes.

6.4 Incident management and breach notification

Syntaq maintains a documented Incident Management policy covering detection, classification, containment, recovery, and post-incident review, with defined severity levels and response times. Where an incident involves personal information and is likely to result in serious harm, Syntaq follows the Notifiable Data Breaches scheme under Part IIIC of the Privacy Act, assessing the breach and notifying the OAIC and affected individuals as required.

6.5 Data retention and deletion

Data is retained only as long as necessary. Active client data and documents are retained for the duration of the contract plus a short defined window, after which they are securely deleted. Audit and security logs follow defined retention periods. Retention is governed by an approved Data Retention Policy aligned to the Privacy Act and applicable record-keeping obligations.

6.6 Supplier and sub processor management

The platforms underpinning Syntaq's services, Microsoft Azure, Vercel, Supabase, and GitHub — are established providers maintaining their own recognised security certifications. Syntaq reviews the continued use and trust posture of these providers at least annually and keeps a current record of any additional service that processes client data.

6.7 People security and awareness

All Syntaq personnel complete security awareness training at least annually and are bound by confidentiality obligations. Access for departing personnel is revoked promptly as part of a defined offboarding process.

7. Specific steps Syntaq takes to safeguard client data

The following is a concise, consolidated summary, suitable for inclusion in your own OAIC or due-diligence documentation, of the concrete measures in place to protect your data:

1. Independently certified our ISMS to ISO/IEC 27001:2022.
2. Encrypt all data in transit using TLS 1.2 minimum and all data at rest using AES-256.
3. Enforce multi-factor authentication on all administrative, deployment, and privileged access.
4. Apply role-based, least-privilege access control with access reviewed at least quarterly.
5. Isolate tenant data using Row Level Security in the managed-service database environment.
6. Store secrets only in protected vaults or server-side encrypted variables, never in code or client bundles.
7. Promote every production change through a reviewed, branch-protected pull request, creating an immutable change record.
8. Run continuous dependency vulnerability scanning and secret scanning, with quarterly vulnerability reviews.
9. Take automated, encrypted backups with point-in-time restore, and test restoration on a defined schedule.
10. Maintain disaster-recovery objectives and test recovery at least annually.
11. Monitor platforms continuously and subscribe to ACSC and vendor threat intelligence.

12. Operate a documented incident-management process aligned to the Notifiable Data Breaches scheme.
13. Retain data only as long as necessary and securely delete it under an approved retention policy.
14. Train all personnel in security awareness annually and bind them to confidentiality obligations.

8. Certifications, standards and contact

- ISO/IEC 27001:2022: certified Information Security Management System (certificate available on request).
- OWASP Top 10: incorporated as a secure-development baseline.
- NIST Cybersecurity Framework: referenced in Syntaq's risk-management approach.
- Compliance alignment: Australian Privacy Act 1988 (Cth) and Australian Privacy Principles; NZ Privacy Act 2020.

For further information, a copy of our ISO 27001 certificate, or to confirm environment-specific details (such as the hosting region for your instance), please contact your Syntaq account manager or the Office of the CTO.