Data Security Policy

Technical and organisational measures for protecting data

[ADOPTIC PTY LTD]

ABN [XX XXX XXX XXX]

Version 1.0 — [DATE]

Confidential

Contents

1. Purpose

This Data Security Policy describes the technical and organisational measures Adoptic employs to protect the confidentiality, integrity, and availability of data processed through the Adoptic platform. It supplements our Privacy Policy and applies to all staff, contractors, and service providers who access or manage Adoptic systems.

2. Scope

This policy covers:

- All Personal Information and Client Data processed through adoptic.online
- All application, assessment, and report data uploaded to or generated by the platform
- All Derived Data produced by Adoptic's analytical processes
- All uploaded documents and files
- All infrastructure, systems, and services used to deliver the platform
- All personnel with access to production systems or client data
- All development, testing, and staging environments that may contain or mirror production data

3. Data Classification

Classification	Description	Handling Requirements
Confidential	Sensitive client data, Personal Information, proprietary application data, Derived Data, uploaded documents, user credentials	Encrypted at rest and in transit; access restricted to authorised personnel; logged access; no sharing outside platform
Internal	Operational data: system configurations, internal notes, analytics, task management, error logs	Access limited to Adoptic personnel; not shared externally without authorisation
Public	Anonymised sample reports, marketing materials, public web pages, this policy	No restrictions on access

All data is treated as Internal by default unless explicitly classified otherwise. Client Data and uploaded documents are always classified as Confidential.

4. Infrastructure Security

4.1 Hosting Environment

Component	Provider	Location	Notes
Application servers	AWS / Railway (transitioning to AWS)	[AWS REGION] / US	Managed cloud infrastructure
Database	PostgreSQL on [AWS RDS / Railway]	[REGION]	Encrypted at rest; automated backups
File storage	[AWS S3 / Platform hosting]	[REGION]	Encrypted at rest; access-controlled
DNS and CDN	[PROVIDER]	Global	DDoS protection

4.2 Network Security

- TLS 1.2+ enforced on all external traffic (HTTPS); HTTP redirected
- Database connections use encrypted transport where supported
- Administrative access restricted by SSH key authentication and IP allowlisting
- No direct public access to database servers or internal services

4.3 Server Hardening

- Operating systems and dependencies kept up to date with security patches
- Unnecessary services and ports disabled
- Production credentials stored in environment variables, never in source code

4.4 Environment Separation

Environment	Purpose	Data
Production	Live platform serving clients	Real client data (Confidential)
Staging	Pre-release testing	Synthetic or anonymised test data only
Development	Local development	Synthetic or anonymised test data only

Real Client Data is never used in staging or development environments without explicit client authorisation and appropriate safeguards.

5. Application Security

5.1 Authentication

- Passwords hashed using PBKDF2 with SHA-256 (via Werkzeug) — never stored, logged, or transmitted in plain text
- Session management uses secure, HTTP-only cookies with CSRF protection
- Account creation is invite-only via secure, time-limited, usage-limited tokens
- Session tokens regenerated on authentication state changes
- [PLANNED] Multi-factor authentication (MFA) support

5.2 Authorisation

- Role-based access control (RBAC) — users assigned roles (admin, staff, viewer) determining permissions
- Organisation-level isolation — client organisations can only access their own data; queries scoped to user's customer memberships
- Principle of least privilege — minimum access required for each role
- Invite management — client administrators control who joins and at what permission level

5.3 Input Validation and Protection

- All database queries use parameterised statements to prevent SQL injection
- Jinja2 auto-escaping prevents Cross-Site Scripting (XSS)
- CSRF tokens validated on all state-changing requests
- File uploads validated for type and size

- [PLANNED] Content Security Policy (CSP) headers
- [PLANNED] Rate limiting on authentication endpoints

5.4 Secure Development Practices

- Source code maintained in version control (Git) with code review
- Secrets and credentials never committed to repositories
- Third-party dependencies reviewed and updated regularly
- [PLANNED] Automated vulnerability scanning (e.g., Dependabot, Snyk)
- [PLANNED] Regular penetration testing by an independent third party

6. Data Protection

6.1 Encryption

State	Method
In transit	TLS 1.2+ (HTTPS) for all browser-to-server and server-to-server communication
At rest	AWS encryption (AES-256) for database volumes and file storage
Passwords	PBKDF2-SHA256 one-way hashing (not reversible)
Backups	Encrypted by hosting provider using provider-managed keys

6.2 Backups

- Database backups performed [FREQUENCY] by the hosting provider
- Backups encrypted and stored in a geographically separate location
- Backup restoration tested [FREQUENCY]
- Backups retained for [PERIOD] before automatic deletion
- Backups subject to the same access controls as production data

6.3 Data Isolation

- Each client's data logically separated using foreign key relationships and application-level access controls
- All queries returning Client Data scoped to the authenticated user's organisation memberships
- Anonymised demonstration data stored separately with no identifying information

- Administrative access to Client Data limited to what is necessary for platform operation

6.4 Document and File Security

- Uploaded documents stored in encrypted storage (e.g., AWS S3 with server-side encryption)
- Access requires authentication and organisation-level authorisation
- [PLANNED] Malware scanning of uploaded files
- [PLANNED] File type restrictions and size limits

7. Data Science and Analytical Processing Security

7.1 Processing Controls

- Analytical processing occurs within the same secured infrastructure as the platform, with the exception of AI/LLM processing which is performed via Amazon Bedrock (see Section 7.5)
- Data transmitted to Amazon Bedrock for AI processing is sent over encrypted channels (TLS) to the Bedrock API within the ap-southeast-2 (Sydney) region
- Processing scripts and algorithms maintained in version-controlled source code
- Changes to analytical algorithms reviewed and tested before deployment
- Processing outputs (Derived Data) subject to the same access controls and classification as input Client Data

7.2 Model and Algorithm Security

- Proprietary algorithms stored in private, access-controlled repositories
- Algorithm parameters, weightings, and configurations classified as Internal
- [PLANNED] Version tracking of model parameters for auditability
- [PLANNED] Bias and fairness monitoring for analytical outputs

7.3 De-identification Standards

When producing aggregated or de-identified data:

- All direct identifiers (names, emails, addresses, organisation names) removed
- Indirect identifiers assessed and suppressed where re-identification risk exists

- Minimum threshold of [X] records before publishing aggregate statistics
- De-identified datasets reviewed before any external use or publication
- Re-identification of individuals prohibited and contractually enforced

7.4 Training Data Governance

- Record maintained of which datasets used for training purposes
- Training data stored separately from production Client Data
- Clients may opt out of de-identified data use for model improvement
- Training data subject to the same retention and disposal policies

7.5 AI/LLM Processing Security

Adoptic's analytical pipeline includes AI processing via Amazon Bedrock, a managed AI service provided by AWS. The following security controls apply to this processing.

Provider security posture:

- Amazon Bedrock is SOC 2 Type II and ISO/IEC 27001 certified
- Data is encrypted in transit (TLS) and at rest by AWS
- AWS does not store, log, or retain input or output data from Bedrock invocations for model training or any other purpose
- Input and output data is not shared with model providers (Anthropic) or across AWS customers — processing is fully isolated per account

Authentication and access:

- Access to the Bedrock API is authenticated via AWS IAM credentials managed by Adoptic
- IAM policies follow least-privilege principles, granting only permissions required for model invocation
- API credentials stored securely in environment variables, never committed to source code

Data residency:

- All AI/LLM processing is confined to the ap-southeast-2 (Sydney, Australia) AWS region
- No Client Data is transferred outside Australia for AI processing

Data handling:

- No persistent storage of inputs or outputs by the LLM provider — data exists only for the duration of each API request
- Ephemeral prompt caching for system prompts only (within-session); cached content is not persisted and is not accessible to other customers

- Each LLM invocation is independent — no data from one client or application is carried over to another

Operational controls:

- Rate limiting implemented on LLM API calls to manage throughput
- Retry logic (up to 3 retries with 30-second delays) handles transient failures
- LLM outputs are validated and structured before incorporation into assessment results
- All LLM invocations logged for audit purposes (request metadata only, not input/output content)

8. Access Control

8.1 Administrative Access

- Production infrastructure access limited to named, authorised Adoptic personnel
- Strong, unique passwords with MFA where available
- Access reviewed [FREQUENCY] and revoked when no longer required
- All administrative actions logged

8.2 Platform Access

- Client administrators control organisation membership and permissions
- Invitation links are single-use or limited-use and time-bound
- Sessions expire after [DURATION] of inactivity
- Consent records maintained with timestamps and IP addresses

8.3 Staff and Contractor Access

- All personnel with data access bound by written confidentiality obligations
- Access granted on a need-to-know, role-specific basis
- Access rights reviewed when staff change roles or leave
- Contractor access is time-limited and expires automatically
- [PLANNED] Background checks for personnel with sensitive data access
- [PLANNED] Regular security awareness training

9. Logging and Monitoring

Event Type	Details Logged
Authentication events	Login attempts (success/failure), logouts, password changes, invitation redemptions
Access events	Pages accessed, reports generated and downloaded, data exports
Administrative actions	User role changes, invitation creation, organisation configuration changes
Data modification	Record creation, updates, and deletions (audit trail)
System events	Server errors, application exceptions, deployment events
Consent events	Consent grants and revocations with timestamps and IP addresses

Logs are stored separately from application data, do not contain passwords or Client Data content, and are retained for [PERIOD] before automatic deletion.

10. Incident Response

Step	Action	Timeframe
1. Identification	Detect and confirm the incident; assign an incident lead	Immediately
2. Containment	Isolate affected systems, revoke compromised credentials	Within hours
3. Assessment	Determine scope, cause, severity; identify affected data and clients	Within 24 hours
4. Notification	Notify affected clients and, where required, regulatory authorities (OAIC, ICO) and affected individuals	Within 72 hours
5. Remediation	Fix root cause, restore systems, implement prevention measures	As soon as practicable
6. Review	Post-incident review; document lessons learned; update policies	Within 30 days

Under the Privacy Act 1988 (Cth), Adoptic is required to notify the OAIC and affected individuals of eligible data breaches likely to result in serious harm. Under UK/EU GDPR, we will notify the relevant supervisory authority within 72 hours and affected individuals without undue delay where the breach poses a high risk.

Where a security incident affects Client Data, we will notify the affected client(s) without undue delay (within 24 hours where practicable), including: the nature of the incident, data affected, measures taken, and recommended actions.

11. Data Retention and Disposal

When data is no longer required:

- Database records are permanently deleted (not merely soft-deleted)
- Uploaded files are removed from storage
- Backups overwritten in the normal rotation cycle
- Cached copies are purged

Client data is deleted or returned upon termination of the client relationship, in accordance with any Data Processing Agreement. Deletion is confirmed in writing upon request.

12. Business Continuity and Disaster Recovery

- Platform hosted on managed cloud infrastructure with [UPTIME SLA] availability
- Database backups enable recovery from data loss or corruption
- Application code maintained in version control for rapid redeployment
- [PLANNED] Documented disaster recovery plan with defined RTO and RPO
- [PLANNED] Regular disaster recovery drills
- [PLANNED] Multi-region failover for high availability

13. Third-Party Risk Management

- Providers assessed for security practices and compliance before engagement
- Providers processing Personal Information subject to Data Processing Agreements
- Contracts restrict providers from using Adoptic data for their own purposes
- Contracts require prompt notification of security incidents
- Current provider list maintained in our Privacy Policy (Section 7.2)
- [PLANNED] Annual review of third-party security practices
- [PLANNED] Right-to-audit clauses in provider contracts

14. Acceptable Use

All users of the Adoptic platform agree to:

- Not attempt to access data belonging to other organisations or users
- Not attempt to circumvent access controls, authentication, or security measures
- Not upload malicious files, code, or content
- Not use the platform for any unlawful purpose
- Not share credentials or allow unauthorised access
- Report any suspected security vulnerabilities or incidents promptly

Violations may result in immediate suspension or termination of access.

15. Compliance

Standard / Regulation	Relevance
Australian Privacy Act 1988 (APPs)	Legal obligation for handling Personal Information in Australia
Notifiable Data Breaches (NDB) scheme	Mandatory breach notification for eligible breaches
UK GDPR / EU GDPR	Applicable where we process data of UK/EEA residents
ISO/IEC 27001:2022	Information security management best practices (aspirational)
OWASP Top 10	Application security baseline
CIS Controls	Infrastructure security best practices (aspirational)

[PLANNED] Formal ISO 27001 certification

[PLANNED] SOC 2 Type II report

16. Policy Review

This policy is reviewed at least annually, or more frequently in response to:

- Significant changes to systems, infrastructure, or analytical processes

- Security incidents or near-misses
- Changes in applicable laws or regulations
- Client or regulatory audit findings
- Addition of new third-party service providers
- Significant changes to data science methodologies or model architectures

Version	Date	Changes
1.0	[DATE]	Initial release

17. Responsibilities

Role	Responsibility
[Privacy/Security Officer]	Owns this policy; oversees security practices, incident response, and compliance
Development team	Implements technical security controls; maintains application and infrastructure security; conducts code reviews
Data science team	Ensures analytical processes comply with this policy; maintains de-identification standards; documents model changes
All staff	Complies with this policy; completes security training; reports suspected incidents promptly

18. Contact

[ADOPTIC PTY LTD]

ABN: [XX XXX XXX XXX]

Email: [SECURITY CONTACT EMAIL]

Website: adoptic.online

To report a security vulnerability, email [SECURITY CONTACT EMAIL] with "Security Vulnerability" in the subject line. We will acknowledge receipt within 1 business day.

This policy was last updated on [DATE].