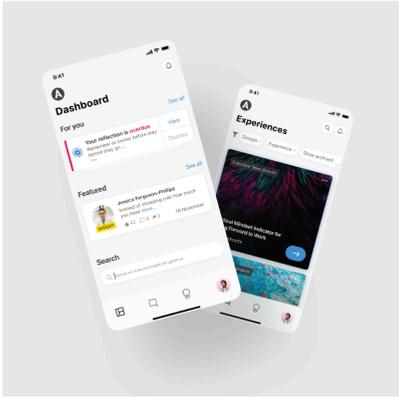


ADEPTION™



Security & Data Privacy Controls Summary

March 2026



Framework Alignment: ISO 27001:2022 | NZ Privacy Act 2020 | GDPR
Trust Center: <https://adeption.io/trust-center>

1. Governance, Risk & Compliance

- **Security Oversight:** Managed by the **Information Security Governance Group (ISGG)**, consisting of the CISO, CTO, and COO.
- **Policies:** Comprehensive suite of formal policies (Access Control, Incident Response, Data Privacy) reviewed annually.
- **Vetting:** Mandatory background checks (Criminal and Address verification) for all personnel with access to production data.
- **Training:** Annual mandatory security awareness training for all staff, including specialized OWASP training for developers.

2. Data Protection & Sovereignty

- **Hosting:** Primary production environment in Microsoft Azure (Dublin, Ireland). Leveraging Tier-1 physical and environmental controls.
- **Encryption:** Data is encrypted at rest using AES-256 and in transit via TLS 1.2+ with modern cipher suites.
- **Credential Security:** Passwords and secrets are never stored in plain text; credentials are hashed and salted using modern cryptographic functions.
- **Sovereignty:** Strict logical separation of data within our multi-tenant architecture.

3. Identity & Access Management

- **Multi-Factor Authentication (MFA):** Mandatory for all administrative and privileged access to the cloud environment and internal tools.
- **Least Privilege:** Access to production data is restricted to authorized personnel only, strictly on a "need-to-know" basis.
- **Review Cycles:** Privileged access rights are reviewed quarterly..

4. Operational Security & Resilience

- **Continuous Monitoring:** Centralized logging and alerting via Microsoft Sentinel for real-time threat detection and anomaly reporting.
- **Vulnerability Management:** Monthly automated scans of internet-facing assets and an annual Independent External Penetration Test.
- **Incident Response:** Formal Cyber Security Incident Response Plan (CSIRP) in place, with a 24-hour notification SLA for critical data breaches.
- **Backups:** Geo-redundant daily backups with a 2-hour Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

5. AI Ethics & Security

- **Proprietary Models:** AI functionality (tool prediction/scoring) is proprietary. We do not transmit customer data to third-party AI/LLM vendors.
- **Privacy-First Training:** No personal information is used to train our AI or machine learning models. All training data is masked and aggregated.

For more information or to request specific audit reports, please visit the [Adeption Trust Center](https://adeption.io/trust-center) or contact our security team at security@adeption.io



Contact

Adeption Information Security
security@adeption.io