Taisen Security FAQ

SECURITY FAQ

FREQUENTLY ASKED QUESTIONS

1.1 General Security

Q: Where is my data stored?

A: Data is stored in secure Google Cloud infrastructure with geographic redundancy. You can specify preferred regions for data storage.

Q: How is my data protected?

A: All data is encrypted both in transit (TLS 1.3) and at rest (AES-256). We implement multiple security layers including WAF, DDoS protection, and secure authentication.

Q: Who has access to my data?

A: Only authorized systems and The Taisen Team for maintenance purposes. All access is logged and monitored.

1.2 Compliance & Privacy

Q: Is Taisen GDPR compliant?

A: Yes, Taisen is fully GDPR compliant and we act as a data processor for our customers. Our DPA incorporates Standard Contractual Clauses for international data transfers.

Q: How do you handle data subject requests?

A: We have procedures in place to assist data controllers in responding to data subject requests for access, rectification, erasure, and data portability.

Q: Are you compliant with Philippine Data Privacy Act?

A: Yes, we are fully compliant with RA 10173 and maintain appropriate security measures for personal data protection.

1.3 Technical Security

Q: What authentication methods do you support?

A: We support multiple authentication methods including email/password, OAuth providers, and API key authentication. Enterprise customers can request SAML SSO integration.

Q: How do you handle security vulnerabilities?
A: We have a vulnerability management program including regular scanning, penetration testing, and a responsible disclosure policy. Critical vulnerabilities are patched immediately.
Q: Do you have a bug bounty program?
A: While we don't have a formal bug bounty program, we welcome responsible disclosure of security vulnerabilities at info.taisernservices@gmail.com.

1.4 Business Security

Q: What is your incident response process?
A: We have documented incident response procedures including detection, analysis, containment, eradication, recovery, and post-incident review.
Q: Do you have business continuity plans?
A: Yes, we maintain business continuity and disaster recovery plans with regular testing and updates.
Q: How do you manage third-party risks?
A: We conduct security assessments of all subprocessors and maintain contractual security requirements with regular monitoring.

IMPLEMENTATION CHECKLIST

SECURITY CONFIGURATION VERIFICATION

2.1 Infrastructure Security

- Cloudflare WAF enabled and configured
- DDoS protection active
- TLS 1.3 enforced
- Security headers implemented
- Rate limiting configured
- Bot management enabled

2.2 Application Security

- Input validation implemented
- Output encoding applied
- Authentication secured
- Session management protected
- API security configured
- Error handling secured

2.3 Data Protection

- Encryption at rest enabled
- Encryption in transit enforced
- Access controls configured
- Data classification implemented
- Backup encryption enabled
- Secure deletion procedures

2.4 Monitoring & Response

- Security logging enabled
- Monitoring configured
- Alerting set up
- Incident response plan
- Regular testing scheduled
- Documentation maintained

CONTACT INFORMATION

Security Inquiries: info.taisernservices@gmail.com

Privacy Questions: info.taisernservices@gmail.com

Technical Support: info.taisernservices@gmail.com

Emergency Security Contact: info.taisernservices@gmail.com

[Subject: SECURITY EMERGENCY - Taisen Search Engine]

DOCUMENT MANAGEMENT

Last Updated: October 26, 2025

Next Review: April 26, 2026

Maintainer: The Taisen Team

Revision History:

- v1.0: Initial Release (January 2024)
- v2.0: Comprehensive Update (October 2025)

This document is provided for informational purposes and represents the security practices of The Taisen Team as of the publication date. Security measures are subject to continuous improvement and may be updated without notice.