Taisen

Security Guidelines

SECURITY GUIDELINES

BEST PRACTICES FOR SECURE USAGE

1.1 API Security

API Key Management:

- Store API keys securely, never in client-side code
- Rotate API keys regularly (recommended every 90 days)
- Use different keys for different environments
- Implement key usage monitoring

Request Security:

- Validate all inputs before sending to Taisen APIs
- Implement request rate limiting on your side
- Use secure connections (HTTPS) for all API calls
- Sanitize search queries to prevent injection attacks

1.2 Data Security

Data Handling:

- Classify data before sending to Taisen
- Implement data minimization principles
- Establish data retention policies
- Secure data in your application before transmission

Transmission Security:

- Ensure your application uses TLS 1.2+
- Validate SSL certificates
- Implement secure WebSocket connections if used
- Monitor for unusual data transmission patterns

1.3 Authentication & Access

User Management:

- Implement strong password policies

- Enable multi-factor authentication where possible
- Use secure session management
- Implement proper logout functionality

Access Controls:

- Follow principle of least privilege
- Regular access reviews
- Secure credential storage
- Audit logging implementation

1.4 Monitoring & Incident Response

Security Monitoring:

- Monitor API usage for anomalies
- Log security events
- Set up alerting for suspicious activities
- Regular security reviews

Incident Response:

- Have a plan for security incidents
- Know how to contact The Taisen Team for security issues
- Understand data breach notification procedures
- Test incident response plans regularly

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)