Security Policy Q&A;

Frequently Asked Questions About Our Security Practices

Last Updated: January 30, 2026
Company: WebShield, Bengaluru, India
Contact: support@webshield.com

General Questions

Q: What is WebShield's Security Policy?

WebShield's Security Policy outlines our comprehensive approach to security, including infrastructure protection, data encryption, access controls, incident response procedures, and our commitment to maintaining the highest security standards to protect user data.

Q: When was the Security Policy last updated?

The Security Policy was last updated on January 30, 2026.

Q: Why is security important for a security platform?

As a cybersecurity platform, we hold ourselves to the highest security standards. We protect sensitive user data and scan results, making our own security practices critical to maintaining user trust and service integrity.

Infrastructure Security

Q: Where is WebShield hosted?

We use enterprise-grade cloud infrastructure with:

- Multi-region deployment for high availability
- Network segmentation and virtual private clouds (VPCs)
- DDoS protection and automated traffic distribution
- Load balancing and auto-scaling capabilities

Q: How does WebShield protect against DDoS attacks?

We implement advanced DDoS protection systems that automatically detect and mitigate distributed denial-of-service attacks to ensure service availability.

Q: What network security measures does WebShield use?

We employ:

- Next-generation firewalls with intrusion detection/prevention (IDS/IPS)
- Network segmentation isolating different service components
- VPN-only access for administrative operations

- Real-time traffic monitoring and analysis

Q: How are WebShield servers secured?

Our servers use:
- Hardened configurations following CIS benchmarks
- Automated security patching and updates
- Minimal attack surface (only essential services)
- Host-based intrusion detection systems (HIDS)
- Regular vulnerability scanning and penetration testing

Data Protection

Q: How does WebShield encrypt data?

We implement comprehensive encryption:
- In Transit: TLS 1.3 with perfect forward secrecy for all data transmission
- At Rest: AES-256 encryption for all stored data, databases, and backups
- End-to-End: Encrypted communication channels for sensitive operations
- Key Management: Secure key storage using hardware security modules (HSMs)

Q: How are passwords stored?

Passwords are hashed using bcrypt with unique salts and a cost factor of 12, making them computationally expensive to crack even if the database is compromised.

Q: Does WebShield check for compromised passwords?

Yes, we use the Have I Been Pwned API to detect if passwords have been exposed in data breaches, protecting users from using compromised credentials.

Q: What happens if I enter the wrong password multiple times?

After multiple failed login attempts, your account is temporarily locked to prevent brute-force attacks. You can reset your password via email.

Q: How does WebShield backup data?

We perform:
- Automated daily backups with encryption
- Geographically distributed backup storage
- Regular backup restoration testing
- Point-in-time recovery capabilities
- 90-day backup retention period

Access Control

Q: What authentication methods does WebShield support?

We support:
- Multi-Factor Authentication (MFA) using TOTP (Time-based One-Time Password)

- Secure session tokens with automatic expiration
- OAuth 2.0 for third-party integrations
- API keys with rate limiting

Q: Should I enable two-factor authentication?

Yes, we strongly recommend enabling 2FA for additional account security. It significantly reduces the risk of unauthorized access even if your password is compromised.

Q: What is Role-Based Access Control (RBAC)?

RBAC is a security model where users are granted permissions based on their roles, ensuring users only have access to data and functions necessary for their job. We follow the principle of least privilege.

Q: How does WebShield control administrative access?

Administrative access requires:

- Mandatory multi-factor authentication
- VPN-only access to production systems
- Comprehensive audit logging of all actions
- Just-in-time (JIT) access provisioning
- Background checks for privileged personnel

Application Security

Q: How does WebShield ensure secure software development?

We follow a Secure Development Lifecycle with:

- Regular security training for developers
- Mandatory peer code reviews
- Automated static code analysis
- Dependency scanning for vulnerable libraries
- Security testing in CI/CD pipeline

Q: Does WebShield protect against OWASP Top 10 vulnerabilities?

Yes, we implement comprehensive protections:

- Injection Prevention: Parameterized queries and input validation
- XSS Protection: Content Security Policy and output encoding
- CSRF Protection: Anti-CSRF tokens for state-changing operations
- Authentication Security: Secure session management and MFA
- And protections against all other OWASP Top 10 threats

Q: How does WebShield protect its API?

Our API security includes:

- Rate limiting to prevent abuse and DDoS
- API key rotation and expiration policies
- Input validation and sanitization
- Comprehensive logging and monitoring
- OAuth 2.0 for third-party integrations

Q: How secure is the WebShield browser extension?

Our browser extension:
- Requests minimal necessary permissions
- Enforces Content Security Policy
- Uses secure communication with backend
- Receives regular security audits and updates
- Is code-signed for authenticity verification

Incident Response

Q: Does WebShield have an incident response plan?

Yes, we maintain a comprehensive 6-phase incident response plan:
1. Detection: 24/7 monitoring and alerting systems
2. Analysis: Rapid assessment of severity and impact
3. Containment: Immediate actions to limit damage
4. Eradication: Removal of threats and vulnerability closure
5. Recovery: Restoration of normal operations
6. Post-Incident: Review and lessons learned

Q: How does WebShield monitor for security threats?

We use:
- SIEM (Security Information and Event Management) for centralized log analysis
- Intrusion Detection Systems for real-time threat detection
- Anomaly Detection using machine learning for behavioral analysis
- Threat Intelligence integration with global threat feeds

Q: Will WebShield notify me if there's a security incident?

Yes, if a security incident affects your data, we will notify you within 72 hours of discovery, providing clear information about the incident and recommended protective measures.

Q: How can I report a security incident?

If you notice suspicious account activity, immediately contact us at support@webshield.com with the subject line "Security Incident".

Vulnerability Disclosure

Q: Does WebShield have a vulnerability disclosure program?

Yes, we welcome security researchers to report vulnerabilities responsibly. We are committed to working with the security community to protect our users.

Q: How do I report a security vulnerability?

Email support@webshield.com with:
- Subject: "Security Vulnerability"
- Detailed information about the vulnerability
- Steps to reproduce the issue

- Allow us reasonable time to fix before public disclosure

Q: What happens after I report a vulnerability?

We will:
- Acknowledge receipt within 48 hours
- Provide regular updates on our progress
- Credit you for responsible disclosure (if desired)
- Not pursue legal action against responsible researchers

Q: Does WebShield have a bug bounty program?

While we don't currently have a formal bug bounty program, we acknowledge responsible disclosures and may offer rewards for critical findings.

Compliance and Certifications

Q: What regulations does WebShield comply with?

We maintain compliance with:
- GDPR (General Data Protection Regulation - EU)
- CCPA (California Consumer Privacy Act)
- IT Act 2000 (Information Technology Act - India)
- CERT-In Guidelines (Indian Computer Emergency Response Team)

Q: What security standards does WebShield follow?

We align with industry-recognized standards:
- OWASP (Open Web Application Security Project) guidelines
- CIS Controls (Center for Internet Security) benchmarks
- NIST Framework (National Institute of Standards and Technology)
- ISO 27001 Information Security Management System (in progress)

Q: Does WebShield undergo security audits?

Yes, we perform:
- Quarterly vulnerability assessments by independent security firms
- Annual penetration testing
- Regular code security audits
- Infrastructure security reviews

User Security Best Practices

Q: How can I keep my WebShield account secure?

Follow these best practices:
- Use a strong, unique password (minimum 12 characters, mixed case, numbers, symbols)
- Enable two-factor authentication (2FA)
- Never share your password or API keys
- Log out from shared or public computers

- Regularly review your account activity

Q: How can I identify phishing attempts?

Be cautious of:
- Unsolicited emails claiming to be from WebShield
- Emails from addresses other than @webshield.com
- Suspicious links or unexpected attachments
- Requests for your password via email (we never ask for passwords)

Q: What should I do if I suspect my account is compromised?

Immediately:
- Change your password
- Check recent account activity
- Contact support@webshield.com with subject "Account Compromise"
- Enable 2FA if not already enabled

Q: Is it safe to install the WebShield browser extension?

Yes, but only install from official browser stores:
- Chrome Web Store
- Firefox Add-ons
- Microsoft Edge Add-ons

Always verify the publisher is "WebShield" before installing.

Security Updates

Q: How often does WebShield apply security updates?

We prioritize security updates:
- Critical vulnerabilities: Addressed within 24 hours
- Dependency updates: Weekly scanning and updating
- Infrastructure patches: Monthly security patches
- Feature updates: Regular releases with security enhancements

Q: Will I be notified of security updates?

Important security updates are communicated via email. For critical updates, we may display in-app notifications.

Q: Does WebShield perform maintenance?

Yes, scheduled maintenance typically occurs during low-traffic periods (02:00-04:00 IST) with advance notice. Emergency maintenance for critical security issues may occur with minimal notice.

Third-Party Security

Q: How does WebShield ensure third-party service security?

We carefully vet all third-party services and ensure they:
- Meet our security standards
- Are contractually bound to protect user data
- Undergo regular security assessments
- Comply with relevant data protection regulations

Q: What third-party services does WebShield use?

We primarily use:
- VirusTotal API for enhanced threat intelligence
- Cloud infrastructure providers for hosting
- Analytics services for service improvement

All are industry-leading services with strong security practices.

Contact Security Team

Q: How can I contact WebShield's security team?

Email support@webshield.com with subject:
- "Security Inquiry" for general questions
- "Security Vulnerability" for vulnerability reports
- "Security Incident" for security concerns

Q: How quickly does WebShield respond to security inquiries?

Security-related inquiries are prioritized and typically responded to within 24 hours.

Q: What is WebShield's company information?

Company Name: WebShield
Location: Bengaluru, India
Contact: support@webshield.com
Security Contact: support@webshield.com (Subject: Security Inquiry)

This document is generated by WebShield and is subject to updates. Please check our website for the most current version.