FuseSign

Security and Compliance

TRUST AT EVERY STEP

www.fusesign.com

Executive Summary

Security, trust, and legal validity are fundamental requirements for electronic signatures used in regulated environments, FuseSign is purpose-built to meet these expectations, delivering enterprise-grade security controls alongside legally recognised electronic signatures globally.

FuseSign combines strong cryptography, secure cloud infrastructure, and trusted certificate authorities to ensure every signed document is tamper-evident, independently verifiable, and defensible over the long term.

This white paper outlines FuseSign's approach to:

1. **Information security governance**
2. **Cryptographic integrity and authentication**
3. **Infrastructure resilience and disaster recovery**
4. **Privacy and regulatory compliance**
5. **Operational transparency and monitoring**

Platform Performance & Reliability

FuseSign operates with high availability and resilience standards suitable for regulated industries.

- Target platform availability: 99.9%
- Average uptime (previous 6 months): 100%
- Over 2,500 customers and 30,000 users supported globally

These metrics reflect FuseSign's commitment to operational continuity and platform stability.

Trust & Adoption

FuseSign is trusted by organisations operating in highly regulated sectors, including financial services, wealth management, insurance, and legal services. The platform has been assessed and approved by major institutions where auditability, enforceability, and technical security controls are mandatory.

FuseSign signatures are automatically trusted in Adobe Acrobat and Adobe Reader through Adobe Approved Trust List (AATL) compliance, allowing signed documents to be independently validated without proprietary tools.

Information Security Governance

FuseSign maintains a formal information security management framework aligned with ISO 27001 principles.
Security governance includes:

- Documented information security policies and procedures
- Role-based access controls for internal systems
- Least-privilege access principles
- Periodic access reviews
- Employee background screening prior to employment
- Mandatory security awareness training at onboarding
- Annual security and privacy refresher training

Access to production systems is restricted to authorised personnel and is logged for audit and review purposes.

Data Security Encryption

FuseSign applies strong cryptographic controls to protect data at rest and in transit.

- AES-256 encryption for data at rest
- TLS 1.2+ encryption for data in transit
- Cryptographic protection applied to signed documents to prevent undetected modification

Each completed document is sealed using digital certificates that ensure integrity and detect tampering.

Access Controls

Access to customer data and administrative systems is controlled using layered security mechanisms.

- Role-based access control (RBAC)
- Least-privilege access enforcement
- Multi-factor authentication (MFA) support
- Logical segregation of customer data within cloud infrastructure

Administrative access is restricted and monitored.

Audit Logging

FuseSign maintains comprehensive audit logging to support evidentiary and compliance requirements.

- Immutable audit trails for signing events
- Detailed event capture including identity verification, timestamps, and IP metadata
- Logs retained in accordance with compliance requirements

Authentication & Signature Integrity

FuseSign provides legally valid electronic signatures using Advanced Electronic Signatures (AdES) under the eIDAS framework.

Security controls include

- Binding of signer identity to each signature
- Cryptographic sealing at the point of signing
- Automatic invalidation if post-signature modification occurs

FuseSign uses qualified certificates issued by GlobalSign, a recognised Qualified Trust Service Provider (QTSP), and supports Long-Term Validation (LTV).

All signatures are

- AATL-compliant
- Automatically trusted in Adobe Acrobat and Reader
- Independently verifiable using embedded cryptographic signatures

Platform Architecture & Hosting

FuseSign is hosted in Australia on Microsoft Azure using enterprise-grade cloud infrastructure.

Infrastructure controls

- Multi-zone redundancy
- Continuous monitoring and alerting
- Azure Defender and centralised logging
- Regular vulnerability management and patching
- Logical segregation of customer environments

Backup, Resilience, & Availability

FuseSign is designed for operational resilience and evidentiary durability.

Security and availability controls include:

- Encrypted backups
- Redundant infrastructure
- Continuous data replication
- Standby recovery environments
- Document immutability

Secure Software Development Lifecycle

Security is embedded into FuseSign's software development lifecycle.

Controls include:

- Secure coding standards
- Peer code review processes
- Automated dependency vulnerability scanning
- Static and dynamic application security testing
- Third-party penetration testing
- Patch management and remediation tracking

All production releases undergo testing prior to deployment.

Disaster Recovery & Business Continuity

FuseSign maintains a tested disaster recovery and business continuity framework designed to protect service availability and data integrity. The platform uses redundant infrastructure, continuous replication, encrypted backups, and controlled recovery procedures to minimise disruption and data loss.

Incident Response & Monitoring

FuseSign maintains defined incident response procedures aligned with regulatory obligations.

- Continuous security monitoring
- Escalation protocols for potential incidents
- Documented response procedures
- Breach notification processes aligned with the Australian Privacy Act and GDPR

Service Communication

FuseSign maintains transparent communication regarding platform performance and updates.
Customers can:

- Access platform updates via the FuseSign knowledge base
- Receive in-application service notifications
- Receive email communications regarding scheduled maintenance or incidents

Service communications are structured to ensure customers are informed of relevant operational events.

Compliance & Certifications

FuseSign aligns with recognised international standards and regulatory frameworks, including:

- ISO 27001 (Information Security Management)
- eIDAS AdES requirements
- GlobalSign qualified certificates
- Adobe AATL compliance
- GDPR (UK and EU)
- Australian Privacy Act

Privacy & Data Ownership

Customers retain full ownership of their data.

FuseSign applies privacy-by-design principles and does not mine, analyse, or resell customer information.

Customer data is processed only for the purpose of delivering the FuseSign service and in accordance with contractual obligations.

Transparency & Verification

Every FuseSign document can be independently verified using:

- Embedded cryptographic signatures
- Adobe-trusted validation mechanisms
- A complete audit history of signing events

This ensures documents remain verifiable and defensible over time.

Conclusion

FuseSign delivers enterprise-grade electronic signatures designed for organisations where security, compliance, and legal defensibility are non-negotiable.

By combining robust cloud infrastructure, strong cryptography, trusted certificate authorities, and structured security governance, FuseSign provides a secure and reliable foundation for executing critical agreements digitally.

FuseSign

E-signing, made easy

Trusted by 2,500+ firms globally

www.fusesign.com