Security Statement

Enterprise-grade security for mission-critical compliance data

Last Updated: November 30, 2025

Certifications & Compliance

ISO 27001

Information Security Management

SOC 2 Type II

Service Organization Controls

NIST 800-171

Controlled Unclassified Information

Security Measures

Data Encryption

All data is encrypted in transit using TLS 1.3 and at rest using AES-256 encryption.

Access Controls

Role-based access control (RBAC) with multi-factor authentication (MFA) required for all users.

Infrastructure Security

Hosted on AWS with redundant systems, DDoS protection, and 99.9% uptime SLA.

Continuous Monitoring

24⁄7 security monitoring, intrusion detection, and automated threat response systems.

Security Training

All employees undergo regular security awareness training and background checks.

Regular Audits

Annual third-party security audits and penetration testing by certified professionals.

Comprehensive Security Framework

1. Data Protection

Intelleges implements multiple layers of data protection to ensure the confidentiality, integrity, and availability of your information:

- **Encryption at Rest:** All data stored in our databases is encrypted using AES-256 encryption
- **Encryption in Transit:** All data transmitted between clients and servers uses TLS 1.3 protocol
- **Database Security:** Encrypted backups, point-in-time recovery, and automated failover
- **Data Segregation:** Logical data separation between customers with strict access controls

2. Access Management

- **Multi-Factor Authentication (MFA):** Required for all user accounts

- **Role-Based Access Control (RBAC):** Granular permissions based on job function
- **Single Sign-On (SSO):** Support for SAML 2.0 and OAuth 2.0
- **Session Management:** Automatic timeout and secure session handling
- **Audit Logging:** Complete audit trail of all access and modifications

3. Infrastructure Security

- **Cloud Provider:** Hosted on AWS with SOC 2 and ISO 27001 certified data centers
- **Network Security:** Virtual Private Cloud (VPC), network segmentation, and firewall rules
- **DDoS Protection:** AWS Shield and CloudFlare protection against distributed attacks
- **Redundancy:** Multi-region deployment with automatic failover
- **Backup & Recovery:** Daily encrypted backups with 30-day retention

4. Application Security

- **Secure Development:** OWASP Top 10 compliance and secure coding practices
- **Code Reviews:** Mandatory peer review and automated security scanning
- **Dependency Management:** Regular updates and vulnerability scanning of third-party libraries
- **Input Validation:** Comprehensive validation and sanitization of all user inputs
- **API Security:** Rate limiting, authentication, and encryption for all API endpoints

5. Monitoring & Incident Response

- **24/7 Monitoring:** Continuous monitoring of systems and security events
- **Intrusion Detection:** Automated detection and alerting of suspicious activities
- **Incident Response Plan:** Documented procedures for security incident handling
- **Breach Notification:** Commitment to notify affected parties within 72 hours
- **Forensics:** Capability to investigate and analyze security incidents

6. Compliance & Governance

- **ISO 27001:** Certified Information Security Management System
- **SOC 2 Type II:** Annual audits of security, availability, and confidentiality controls
- **GDPR Compliance:** Full compliance with EU data protection regulations
- **CCPA Compliance:** California Consumer Privacy Act compliance
- **NIST 800-171:** Compliance with Controlled Unclassified Information requirements

7. Physical Security

- **Data Center Security:** AWS data centers with 24/7 physical security
- **Access Controls:** Biometric access and video surveillance
- **Environmental Controls:** Fire suppression, climate control, and power redundancy
- **Asset Disposal:** Secure destruction of hardware according to NIST guidelines

8. Employee Security

- **Background Checks:** All employees undergo comprehensive background verification
- **Security Training:** Regular security awareness and compliance training
- **Confidentiality Agreements:** All employees sign NDAs and security policies
- **Least Privilege:** Employees have access only to data required for their role

9. Third-Party Security

- **Vendor Assessment:** Security evaluation of all third-party service providers
- **Data Processing Agreements:** Contractual security and privacy requirements
- **Regular Reviews:** Ongoing monitoring of third-party security posture

10. Business Continuity

- **Disaster Recovery Plan:** Documented procedures for service restoration

- **Backup Strategy:** Automated daily backups with geographic redundancy
- **Uptime SLA:** 99.9% availability guarantee
- **Failover Testing:** Regular testing of disaster recovery procedures

Responsible Disclosure Policy

Intelleges is committed to working with security researchers to identify and resolve security vulnerabilities. If you believe you have discovered a security issue, please report it to our security team:

Email: security@intelleges.com
PGP Key: Available upon request
Response Time: We aim to acknowledge reports within 24 hours

Please provide detailed information about the vulnerability, including steps to reproduce. We request that you do not publicly disclose the issue until we have had an opportunity to address it.

Questions About Our Security?

Our security team is available to answer questions and provide additional documentation.

Security Team: security@intelleges.com
Compliance Team: compliance@intelleges.com

ISO 27001 Certified | Battelle Supplier of the Year