Security Information

aeShield® is a web based application end users access through their browser. With both SaaS or On-Prem solutions to choose from, you can be sure to have the right fit for your organization. The aeShield team follows documented policies designed to comply with ISO 27001. Employees are trained regularly on confidentiality and information security.

Compliance Made Simple

Personal Data Handling

aeShield maintains only minimal PII limited to names, emails and passwords. Controls are in place to comply with GDPR. Authentication is secured by MFA using TOTP.

Infrastructure Safeguards

Hosted in a SOC 2 Type II Certified Data Center ensuring physical and logical controls for security. A Managed Detection and Response is deployed and maintained for all servers and endpoints. Firewall maintained with DDoS protection.

Disaster Recovery

A geographically diverse failover location is maintained with mirroring every 15 minutes to provide reliable hosting in event of physical challenge to the datacenter. RTO of 4 hours and RPO of 60 minutes to keep you up and running. Disaster Recovery plan is reviewed and tested annually.

Incident Response Plan

Documented Incident Response Plan includes communication requirements to any affected parties within 24 hours of identified incident. 90 day backups maintained to aid in investigation, containment, eradication and recovery.

Data Integrity

All data is encrypted in transit and at rest. Principle of Least Privilege employed within the aeShield application and for all internal systems. aeShield supports role based permissions allowing your system administrators to customize those permissions as required. Client data is maintained in dedicated databases.

Contact Us www.aeShield.com +1 (864) 404-3082 info@aeShield.com