

Security Policy

SentraShield Internal Document — Confidential

Data Encryption at Rest

SentraShield encrypts all customer data at rest using AES-256 encryption. This standard is applied across all storage layers including primary databases, backup stores, and file systems. Encryption keys are managed using AWS Key Management Service (KMS) and rotated annually.

Data Encryption in Transit

All data transmitted between clients and SentraShield servers is encrypted using TLS 1.2 or higher. Older protocols including TLS 1.0 and TLS 1.1 are explicitly disabled. HTTPS is enforced for all API endpoints and web interfaces.

Multi-Factor Authentication

Multi-factor authentication (MFA) is mandatory for all administrative accounts and strongly recommended for all end users. Supported MFA methods include Time-Based One-Time Passwords (TOTP) via authenticator apps and hardware security keys (FIDO2/WebAuthn compliant).

Access Control Policy

SentraShield enforces Role-Based Access Control (RBAC) across all internal systems and customer-facing platforms. Employees are granted access based on the principle of least privilege — access is limited to what is strictly necessary to perform their role. All access permissions are reviewed quarterly by department managers and the security team. Access is revoked immediately upon employee offboarding.

Password Policy

All internal accounts must use passwords of at least 14 characters, containing a mix of uppercase, lowercase, numbers, and special characters. Passwords must be changed every 90 days. Password reuse for the last 10 passwords is prohibited.