Data security policy (high level)

Objective
Protect company and partner data from unauthorized access, disclosure, alteration, and destruction.

Key controls
- Access control: least privilege for systems and sensitive data.
- Authentication: strong passwords and mandatory 2FA for staff access.
- Encryption: TLS for network traffic; encryption at rest for sensitive stores.
- Backups: automated backups with restricted access and periodic restore tests.
- Vulnerability management: scheduled patching and dependency scanning.
- Incident response: documented plan with roles and notification procedures.

Developer practices
- Code reviews, dependency scanning, and secrets scanning in CI.
- No hard-coded secrets; use secret management solutions.
- Logging and monitoring to detect unusual activity.

Third-party vendors
- Security assessments and contractual safeguards before onboarding processors.
- Minimum security requirements included in vendor selection.