Regulations (Small Dummy)

Compliance Regulations (Dummy) - Version 1.0

Section 1: Data Protection
R1.1 Personal data must be encrypted at rest using industry-standard encryption (e.g., AES-256).
R1.2 Personal data must be encrypted in transit using TLS 1.2 or higher.
R1.3 Access to personal data must be controlled using role-based access control (RBAC).
R1.4 Only authorized personnel may access customer personal data and access must be logged.
R1.5 Data retention must not exceed 180 days unless required by law or contract.
R1.6 Data subjects must be able to request deletion of personal data, processed within 30 days.

Section 2: Security Operations
R2.1 Systems must maintain audit logs for sensitive actions (admin login, data export, privilege changes).
R2.2 Audit logs must be retained for a minimum of 90 days and protected from tampering.
R2.3 Multi-factor authentication (MFA) must be enabled for all admin accounts.
R2.4 Security patches must be applied at least monthly.
R2.5 Incident response procedures must be documented; notify customer within 72 hours of breach.

Section 3: Third Parties
R3.1 Customer data must not be shared with third parties without written consent.
R3.2 All third-party processors must sign a Data Processing Agreement (DPA).
R3.3 Third-party data sharing must be disclosed in a privacy policy and vendor list.
R3.4 Sub-processors require prior notice and an option for customer objection.

Section 4: Governance
R4.1 A security contact must be designated and reachable for security inquiries.
R4.2 Annual security training is required for staff with access to customer data.
R4.3 Backups must be encrypted and tested quarterly for restorability.