All customer personal data must be encrypted at rest and in transit using AES-256 encryption.

Access to production servers is restricted only to authorized DevOps personnel. Unauthorized access is prohibited.

Code changes must go through quality assurance and staging environments before being deployed to production servers.

Customer data cannot be copied, downloaded, or transferred to local machines, devices, or any non-authorized third party system.

Sharing of credentials including passwords, API keys, SSH keys, and access tokens between users, even internal team members, is strictly prohibited.

All administrator activities like server restarts, configuration changes, account control changes must be logged with audit trail tracking user, timestamp, changes made, and authorization.

Financial transactions over $10,000 require dual authorization using multi-factor authentication for enhanced security.

Regular security audits will be conducted to ensure compliance with all policies and procedures. Violations may result in disciplinary action.