Company Information Security Policy

1. Data Retention Policy
All employee and customer data must be retained for a minimum period of 5 years.
After the retention period, data must be securely deleted or anonymized.

2. Access Control
Access to internal systems is granted based on role-based access control (RBAC).
Employees must not share credentials under any circumstances.

3. Password Policy
Passwords must be at least 12 characters long and include uppercase, lowercase,
numbers, and special characters. Passwords must be changed every 90 days.

4. Incident Reporting
Any security incident must be reported to the IT Security Team within 24 hours.