Corporate Information Security Policy

1. Introduction

This Security Policy outlines the company’s approach to protecting sensitive information and ensuring compliance with applicable regulations including GDPR and CCPA.

2. Data Protection

All personal data must be processed lawfully, fairly, and transparently. Data shall only be collected for specified and legitimate purposes.

3. Access Control

Access to sensitive systems shall be restricted to authorized personnel only. Role-based access control (RBAC) must be implemented.

4. Encryption Policy (Needs Improvement)

Sensitive data should ideally be encrypted where possible. However, encryption standards are not clearly defined in this document.

5. Incident Response (Incomplete)

Security incidents should be reported to management. Detailed breach notification timelines and regulatory reporting procedures are not specified.

6. Data Retention

Personal data shall not be retained longer than necessary. Retention periods must be reviewed annually.

7. Conclusion

This policy is subject to annual review. Departments must ensure adherence to this document to maintain compliance and data security standards.