IT Policies - Data Privacy

Data Privacy Policy:

Purpose:

- Ensure compliance with data protection laws including GDPR and CCPA.

Data Collection:

- Collect only necessary personal data, clearly informing individuals of the use and duration of storage.

Data Storage:

- Data stored securely in encrypted databases.
- Regular audits and vulnerability assessments conducted.

Employee Responsibilities:

- Employees must complete annual data privacy training.
- Reporting data breaches immediately to IT Security.

Access Control:

- Role-based access control enforced strictly.
- Regular reviews of access permissions.

Third-party Data Handling:

- Contracts with third parties include strict data privacy clauses and audit rights.

Incident Response:

- Clear protocols for responding to data breaches, including notification and mitigation strategies.

IT Policies - Password Management

Password Management Policy:

Password Requirements:
- Minimum of 12 characters including uppercase, lowercase, numbers, and special characters.
- Avoid common words or easily guessed information.

Frequency:
- Passwords must be changed every 90 days.
- Systems enforce automatic reminders.

Multi-Factor Authentication (MFA):
- Mandatory MFA implementation on all systems handling sensitive information.

Account Security:
- Accounts automatically locked after 5 unsuccessful login attempts.
- Users must contact IT support to regain access.

Password Storage:
- Passwords must never be written down or shared.

Password Management Tools:
- Use of approved password managers recommended.
- Regular audits to detect weak or compromised passwords.

Compliance and Enforcement:
- Violations lead to disciplinary action, including possible termination.

IT Policies - Device Usage

Device Usage Policy:

Device Approval:

- Employees must use only approved devices for work-related tasks.

Security Standards:

- Devices must be password protected and equipped with antivirus software.
- Automatic updates and security patches must be enabled.

Personal Devices (BYOD):

- Permitted only with IT approval, subject to additional security controls and monitoring.

Prohibited Activities:

- Unapproved software installation.
- Accessing or storing inappropriate or illegal content.

Data Handling on Devices:

- Employees must encrypt sensitive data stored on devices.
- Regular backups required to prevent data loss.

Incident Reporting:

- Loss, theft, or compromise of devices must be reported immediately.

Device Return Policy:

- Upon termination or resignation, devices must be returned promptly.