Project 3: Policy Documents

1️⃣ Password Policy

ABC Tech Pvt Ltd – Password Policy

Purpose:
To ensure all employees use strong, secure passwords to protect company systems and data.

Scope:
This policy applies to all employees, contractors, and temporary staff accessing company systems.

Policy:
1. Passwords must be at least 12 characters long.
2. Must include uppercase, lowercase, numbers, and special characters.
3. Passwords must not be shared with anyone.
4. Multi-Factor Authentication (MFA) must be enabled wherever possible.
5. Passwords must be changed every 90 days.
6. Default passwords on devices or software must be changed immediately.

Responsibilities:
- Employees must follow this policy and report any password-related incidents.
- IT/Compliance team will monitor compliance and enforce password rules.

Review:
This policy will be reviewed annually or after a security incident.

2️⃣ Email / Communication Policy

ABC Tech Pvt Ltd – Email & Communication Policy

Purpose:
To ensure safe and professional use of company email and communication tools.

Scope:
Applies to all employees, contractors, and temporary staff using company email or communication platforms.

Policy:
1. Company email must be used for work-related communication only.
2. Do NOT share confidential company information outside the organization without authorization.
3. Avoid clicking on links or attachments from unknown sources.
4. Always verify email sender identity if requesting sensitive information.
5. Use professional language and tone in all communication.

Responsibilities:
- Employees must follow safe email practices and report suspicious emails.
- Compliance/IT team monitors and enforces email security practices.

Review:
This policy will be reviewed annually.

3️⃣ Data Handling / Acceptable Use Policy

ABC Tech Pvt Ltd – Data Handling & Acceptable Use Policy

Purpose:
To ensure proper handling of sensitive and confidential data and acceptable use of company resources.

Scope:

Applies to all employees, contractors, and temporary staff accessing company data or IT resources.

Policy:

1. Only access data required for your job role.
2. Confidential data must not be shared with unauthorized persons.
3. Store data securely (encrypted or in designated storage systems).
4. Company devices must not be used for personal, illegal, or unauthorized purposes.
5. Any suspected data breach must be reported immediately to Compliance/IT team.

Responsibilities:

- Employees must handle data responsibly and report incidents.
- IT/Compliance team ensures compliance with this policy.

Review:

Policy reviewed annually or after security incidents.