Security Policy Drafts

1. Password Policy

Purpose: Ensure strong authentication practices.

Requirements:

- Passwords must be minimum 12 characters long
- Must include uppercase, lowercase, numbers, and symbols
- Prohibit reuse of last 5 passwords
- Mandatory password changes every 90 days
- Multi-Factor Authentication (MFA) required for all privileged accounts

Enforcement: Accounts will be locked after 5 failed login attempts. Violations may result in suspension.

2. Acceptable Use Policy (AUP)

Purpose: Define acceptable behavior when using organizational IT resources.

Requirements:

- Company resources may not be used for illegal, malicious, or non-business purposes
- Users must not disable security controls (e.g., antivirus, firewalls)
- Installation of unauthorized software is prohibited
- Sensitive data must not be stored on personal devices without encryption
- Internet usage is subject to monitoring for compliance

Enforcement: Breaches may result in disciplinary action, including termination.

3. Data Handling & Classification Policy

Purpose: Protect sensitive data in line with regulatory and business requirements.

Classification Levels:

- Public – Information freely shareable with the public
- Internal Use Only – Non-sensitive data limited to employees
- Confidential – Customer, financial, or proprietary data
- Restricted – Highly sensitive (PII, payment card data, healthcare data)

Handling Requirements:

- Confidential/Restricted data must be encrypted at rest and in transit
- Access based on principle of least privilege
- External sharing of Confidential/Restricted data requires management approval and secure transfer methods

Enforcement: Violations may trigger incident response investigation and compliance reporting.