Policy 03: IT Security & Compliance

Effective Date: January 1, 2024

1. Password Policy
- Minimum length: 12 characters.
- Complexity: Must include uppercase, lowercase, numbers, and symbols.
- Rotation: Passwords must be changed every 90 days.

2. Multi-Factor Authentication (MFA)
- MFA is mandatory for all internal systems (Email, GitHub, AWS, HR Portal).
- Use of an authenticator app (e.g., Google Authenticator, Authy) is preferred over SMS.

3. Device Security
- Laptops must be encrypted (FileVault/BitLocker).
- Screen lock must activate after 5 minutes of inactivity.
- Do not leave devices unattended in public spaces.

4. Data Handling
- Customer data must never be stored on local machines.
- Use approved encrypted channels for sharing sensitive credentials.