Policy 03: IT Security, Data Protection & Compliance

Effective Date: January 1, 2024
Document Owner: CISO (Chief Information Security Officer)
Version: 4.2

1. Password & Authentication Standards
1.1 Password Complexity
- Minimum length: 14 characters (expanded from previous 12).
- Must contain a mix of uppercase, lowercase, numbers, and special symbols.
- Passwords must not contain common dictionary words or personal info (e.g., "Password123", "PracticalAI").

1.2 Rotation & History
- Passwords must be rotated every 90 days.
- You cannot reuse the last 5 passwords.

1.3 Multi-Factor Authentication (MFA)
- MFA is MANDATORY for all internal systems including Google Workspace, AWS, GitHub, Slack, and HR portals.
- Hardware keys (YubiKeys) or TOTP apps (Google Authenticator, Authy) are the only approved methods. SMS-based MFA is p

2. Device Security (Endpoint Protection)
2.1 Encryption
- All company laptops must have Full Disk Encryption enabled (FileVault for Mac, BitLocker for Windows).
- Mobile devices accessing company email must be enrolled in MDM (Mobile Device Management).

2.2 Physical Security
- Screen lock must be set to activate after a maximum of 5 minutes of inactivity.
- Devices must never be left unattended in public vehicles or spaces.
- Lost or stolen devices must be reported to IT Security immediately (within 1 hour).

2.3 Software Installation
- Users do not have local Admin rights by default.
- Only software from the "Self Service" portal or approved by IT may be installed.
- Shadow IT (unapproved SaaS tools) is strictly prohibited.

3. Data Handling & Classification
3.1 Data Classification Levels
- Public: Marketing materials, job descriptions.
- Internal: Policies, memos, org charts.
- Confidential: Customer lists, pricing strategies, source code.
- Restricted: PII (Personally Identifiable Information), financial records, private keys.

3.2 Storage & Transfer
- Customer data must NEVER be stored on local laptop drives. It must remain in approved cloud databases (AWS RDS, S3) wit
- Do not use personal email or personal cloud storage (Dropbox, GDrive) for company data.
- Sensitive credentials (API keys, passwords) must be shared via 1Password, never via Slack or Email.

4. Acceptable Use
- Company devices are tools for business. Incidental personal use is permitted if it does not interfere with productivity or security

- Accessing illegal, adult, or gambling content is strictly prohibited and is grounds for immediate termination.
- Do not connect unknown USB drives or peripherals to company machines.

5. Incident Response
- If you suspect a breach, phishing attempt, or malware infection, disconnect from the network and contact the Security Operatio
- Do not attempt to investigate the breach yourself.

6. Remote Access (VPN)
- Access to internal staging/production environments requires connection via the corporate VPN (WireGuard).
- VPN access is logged and monitored for anomalous behavior.