**📘 IT, Security & Compliance Policies**

**1. Introduction**

**Technology is the backbone of modern work. This handbook defines how employees must use IT systems responsibly, protect company data, and respond to security threats. It blends policies (rules that must be followed) with best practices (recommended ways of working).**

**Our IT & Security principles:**

1. **Confidentiality – protect sensitive information.**
2. **Integrity – maintain accuracy and reliability of data.**
3. **Availability – ensure systems are accessible when needed.**
4. **Accountability – every employee is responsible for safeguarding data.**

**2. Acceptable Use Policy**

**Employees must use IT resources for legitimate business purposes.**

**Permitted Use**

* **Accessing work email, Slack, and approved apps.**
* **Researching industry trends.**
* **Limited personal use (e.g., checking personal email at lunch).**

**Prohibited Use**

* **Installing unauthorized software.**
* **Visiting malicious or inappropriate websites.**
* **Using corporate email for personal business.**
* **Sharing company data with third parties without approval.**

**📌 Case Example:  
An employee downloads free video editing software on a company laptop. The software contains spyware, leading to a data breach. → Result: disciplinary action + reminder to install only IT-approved tools.**

**3. Authentication & Password Policy**

**Passwords are the first line of defense.**

**Password Requirements**

* **Minimum length: 12 characters.**
* **Must include uppercase, lowercase, number, symbol.**
* **No reuse of last 5 passwords.**
* **Must not include personal info (birthdate, pet names).**

**Multi-Factor Authentication (MFA)**

* **Required for VPN, email, HR, and financial systems.**
* **Options: Authenticator app, hardware token, SMS (last resort).**

**Best Practices**

* **Use a password manager (e.g., 1Password, Bitwarden).**
* **Change master password every 6 months.**
* **Do not write passwords on sticky notes.**

**4. Device & Endpoint Security**

**Company Devices**

* **Pre-installed antivirus & endpoint protection (auto-updates).**
* **Full-disk encryption (BitLocker, FileVault).**
* **IT must approve all software installs.**

**Bring Your Own Device (BYOD)**

* **Allowed only if enrolled in Mobile Device Management (MDM).**
* **Devices must have:**
  + **Latest OS updates**
  + **Encrypted storage**
  + **Remote wipe enabled**

**📌 Scenario:  
John accesses work email from his personal phone without encryption. The phone is stolen. Because he didn’t enable remote wipe, sensitive data is compromised. → Disciplinary action + security retraining.**

**5. Data Protection & Privacy**

**We follow GDPR, CCPA, and other regional data laws.**

**Data Classification**

* **Confidential: HR records, financial data, source code.**
* **Internal: team strategies, project documents.**
* **Public: published blogs, press releases.**

**Data Handling Rules**

| **Classification** | **Storage** | **Sharing** | **Retention** |
| --- | --- | --- | --- |
| **Confidential** | **Encrypted drives** | **Restricted access** | **7 years** |
| **Internal** | **Shared drives (access-controlled)** | **Internal only** | **3 years** |
| **Public** | **Open repositories** | **Public channels** | **Indefinite** |

**Employee Responsibilities**

* **Do not send confidential data over personal email.**
* **Report misdirected emails immediately.**
* **Use secure transfer tools (SFTP, encrypted email).**

**6. Network & Remote Access**

**VPN Policy**

* **Mandatory for remote access to internal systems.**
* **Split tunneling disabled to prevent data leakage.**

**Wi-Fi Security**

* **Use WPA3 or WPA2 at minimum.**
* **Avoid public Wi-Fi (use mobile hotspot + VPN).**

**📌 Case Example:  
Employee uses café Wi-Fi to log into CRM without VPN. A hacker intercepts the session → customer data leak.**

**7. Incident Management**

**Employees are the first line of defense in reporting incidents.**

**What to Report**

* **Phishing emails.**
* **Suspicious logins (unknown devices/IPs).**
* **Lost or stolen devices.**
* **Malware alerts.**

**Reporting Process**

1. **Contact IT via Security Hotline (24/7).**
2. **Fill out Incident Report Form.**
3. **IT triages: Low / Medium / High / Critical.**
4. **Response team investigates & remediates.**

**Example: Phishing**

**An employee receives an email: *“Reset your payroll password here.”* They click the link but do not enter credentials. They report it → IT quarantines the domain → company avoids compromise.**

**8. Backup & Disaster Recovery**

**Backup Standards**

* **Servers: nightly full backup + hourly incremental.**
* **Laptops: daily cloud sync (OneDrive/Google Drive).**
* **Databases: real-time replication.**

**Disaster Recovery (DR)**

* **RTO (Recovery Time Objective): 4 hours.**
* **RPO (Recovery Point Objective): 30 minutes.**
* **Annual DR drills with mock outage scenarios.**

**📌 Scenario:  
Primary data center outage due to fire. DR site activated in 2 hours, services restored with <15 min data loss.**

**9. Physical Security**

**Even digital security depends on physical safeguards.**

* **Badge access required in office.**
* **Visitors must sign in and wear badges.**
* **No “tailgating” (following someone into secure areas).**
* **Servers locked in restricted-access rooms.**

**10. Compliance & Auditing**

**We comply with:**

* **ISO 27001 – Information Security Management.**
* **SOC 2 – Controls for data handling.**
* **GDPR/CCPA – Data protection laws.**

**Audits are conducted annually, and employees may be asked to provide evidence (e.g., screenshots of encrypted devices).**

**11. Security Awareness & Training**

* **Mandatory annual training for all employees.**
* **Quarterly phishing simulations.**
* **Security champions in each department.**

**📌 Example:  
Quarterly phishing simulation → 5% employees clicked link. Follow-up training reduced rate to 1% over 6 months.**

**12. Emerging Technology Policy**

* **AI & Automation: Use approved AI tools, do not upload confidential data into ChatGPT/public AI.**
* **IoT Devices: Must be registered with IT.**
* **Cloud Services: Only IT-approved SaaS tools allowed. Shadow IT is prohibited.**

**13. Enforcement & Disciplinary Action**

**Non-compliance may result in:**

* **Verbal/written warning.**
* **Removal of IT access.**
* **Termination for gross negligence.**

**14. Policy Review & Governance**

* **Policy reviewed every 12 months.**
* **Major incidents may trigger immediate revision.**
* **Updates communicated via company-wide email.**