**IT, Data Security & Privacy Policy**

**1. Purpose**

The purpose of this policy is to safeguard the company’s information assets, IT systems, networks, and data. It establishes standards for secure, responsible, and compliant use of technology resources while protecting proprietary, confidential, and personal information.

**2. Scope**

This policy applies to all employees, contractors, interns, consultants, and third-party vendors who have access to company IT resources or handle sensitive company data. It covers hardware, software, networks, emails, cloud services, mobile devices, and remote work systems.

**3. Acceptable Use of IT Resources**

**3.1 General Guidelines**

* IT resources are provided for business purposes only.
* Personal use should be minimal and should not affect productivity or security.

**3.2 Prohibited Activities**

* Unauthorized access to company or third-party systems.
* Installing unlicensed software or applications.
* Sharing passwords or accounts.
* Downloading malicious or pirated software.
* Using company systems for illegal or unethical activities.

**3.3 User Responsibilities**

* Protect account credentials and devices.
* Report lost or stolen devices immediately.
* Follow all IT security protocols.

**4. Device & Endpoint Security**

**4.1 Company-Provided Devices**

* Laptops, desktops, and mobile devices must be configured with company-approved security software.
* Antivirus, firewall, and endpoint protection must remain active at all times.

**4.2 Bring Your Own Device (BYOD)**

* Allowed only with IT approval and compliance with company security standards.
* Company data accessed on personal devices must be encrypted and secured.

**4.3 Mobile Device Management (MDM)**

* Mobile devices must use secure passwords, biometrics, and approved applications.
* Lost devices must be reported immediately to IT for remote lock or wipe.

**5. Network & VPN Security**

**5.1 Office Network Usage**

* All network access must comply with company IT policies.
* Unauthorized devices or routers are prohibited.

**5.2 Remote Work Access**

* VPN access is mandatory for accessing company systems remotely.
* Avoid public Wi-Fi unless using company-approved VPN and secure endpoints.

**5.3 Monitoring & Auditing**

* Company reserves the right to monitor network traffic, email communications, and system access.
* Monitoring is conducted to detect policy violations and security threats.

**6. Data Protection & Privacy**

**6.1 Confidential Information**

* Protect proprietary, financial, client, and employee information.
* Share confidential data only with authorized personnel via secure channels.

**6.2 Personal Data Compliance**

* Employees must handle personal data in compliance with GDPR, local laws, and company standards.
* Access to sensitive personal data requires authorization and audit trails.

**6.3 Data Storage & Retention**

* Data must be stored on approved servers or cloud services.
* Retention periods follow legal and business requirements.
* Secure disposal is required for obsolete data.

**7. Email, Communication & Collaboration Tools**

**7.1 Email Use**

* Emails must be professional, accurate, and relevant to business purposes.
* Avoid sharing sensitive information via personal email accounts.

**7.2 Collaboration Platforms**

* Use approved communication and project management tools.
* Sensitive discussions should occur on secure, encrypted channels.

**7.3 External Communication**

* Employees representing the company must follow approved guidelines.
* No confidential information should be shared externally without authorization.

**8. Incident Reporting & Response**

**8.1 Reporting Security Incidents**

* Report any suspected breach, phishing attempt, or malware immediately to IT Security.
* Examples: Unauthorized access, stolen devices, suspicious emails, data leaks.

**8.2 Incident Response Procedure**

1. Employee reports incident via IT portal or hotline.
2. IT assesses severity and classifies the incident.
3. Containment measures are taken (e.g., account lock, system isolation).
4. Investigation identifies root cause and impacted data.
5. Remediation steps are applied and documented.
6. Affected stakeholders are notified if necessary.

**8.3 Follow-up & Training**

* Post-incident analysis may result in policy updates, additional training, or technical improvements.

**9. Training & Awareness Programs**

**9.1 Mandatory Training**

* All employees must complete IT security and privacy training upon joining and annually.

**9.2 Awareness Campaigns**

* Periodic emails, webinars, and workshops to highlight new threats, phishing attacks, and best practices.

**9.3 Accountability**

* Non-compliance with training or security practices may result in disciplinary action.

**10. Practical Examples & Case Studies**

**Example 1:**  
An employee receives a suspicious email requesting credentials. They report it to IT, preventing a potential breach. Training reinforced proper email verification procedures.

**Example 2:**  
A remote employee’s laptop is stolen. IT remotely wipes the device, preventing data exposure. A case study on BYOD security is shared with the team.

**Example 3:**  
Unauthorized software installation is detected during routine audit. Employee receives counseling and a written warning.

**11. FAQs**

**Q1:** Can I use my personal device for work?  
**A:** Only with IT approval and compliance with security protocols.

**Q2:** What if I notice a data breach?  
**A:** Report immediately to IT Security; follow incident reporting procedure.

**Q3:** Are emails monitored?  
**A:** Yes, to ensure compliance with company policy and security standards.

**Q4:** How often should passwords be changed?  
**A:** As per IT guidelines, typically every 90 days.