**IT POLICY MANUAL**

**I. PURPOSE**  
This policy is designed to outline the rules and regulations for the use of IT resources within the company. It aims to ensure the secure, efficient, and responsible use of all IT assets.

**II. SCOPE**  
This policy applies to all employees, contractors, consultants, temporary workers, and other workers, including all personnel affiliated with third parties who access the company’s IT systems.

**III. IT POLICY**

**A. Acceptable Use Policy**

1. **Scope:** This policy applies to the use of all company IT resources, including but not limited to computers, networks, email systems, and internet access.
2. **Purpose:** To ensure that all IT resources are used responsibly, legally, and in a manner that does not compromise the integrity or security of the company’s information.
3. **Guidelines:**
   * Employees must use IT resources primarily for business purposes.
   * Personal use should be limited and should not interfere with job performance or violate any other company policies.
   * The installation of unauthorized software or hardware is prohibited.
   * The use of company IT resources for illegal activities, harassment, or any form of inappropriate behavior is strictly forbidden.
   * Employees should not access, download, or distribute any material that is illegal, offensive, or discriminatory.

**B. Data Security and Privacy Policy**

1. **Scope:** This policy applies to all data, whether stored digitally or physically, that the company processes.
2. **Purpose:** To protect the confidentiality, integrity, and availability of company data.
3. **Guidelines:**
   * Employees must follow all company procedures for the secure storage, transmission, and disposal of data.
   * Personal data of employees, customers, and business partners must be handled in accordance with data protection laws.
   * Access to sensitive data is restricted to authorized personnel only.
   * All data breaches or security incidents must be reported immediately to the IT department.

**C. Password Management Policy**

1. **Scope:** This policy applies to all systems and applications that require authentication.
2. **Purpose:** To enforce strong password practices across the company.
3. **Guidelines:**
   * Passwords must be a minimum of 8 characters in length and include a mix of letters, numbers, and special characters.
   * Passwords must be changed every 90 days.
   * Employees must not share their passwords with anyone.
   * Multi-factor authentication (MFA) is required for access to sensitive systems.

**D. Internet and Email Policy**

1. **Scope:** This policy applies to the use of the company’s internet and email systems.
2. **Purpose:** To regulate the use of internet and email to ensure they are used effectively for business purposes.
3. **Guidelines:**
   * The company’s email system should be used for business-related communications only.
   * Personal use of the internet should be minimal and should not affect productivity.
   * The company reserves the right to monitor internet usage and email communications.
   * Employees must not send or forward chain letters, spam, or inappropriate content.

**E. Software Management Policy**

1. **Scope:** This policy applies to all software used within the company.
2. **Purpose:** To ensure that all software is properly licensed and maintained.
3. **Guidelines:**
   * Only authorized software approved by the IT department may be installed on company devices.
   * The use of unlicensed or pirated software is strictly prohibited.
   * Software updates and patches must be installed as soon as they are released.

**F. Hardware Management Policy**

1. **Scope:** This policy applies to all hardware owned or leased by the company.
2. **Purpose:** To manage and protect the company’s IT hardware assets.
3. **Guidelines:**
   * All hardware must be approved by the IT department before purchase.
   * Employees are responsible for the care and protection of company hardware in their possession.
   * Lost or stolen hardware must be reported to the IT department immediately.

**G. Remote Work and Bring Your Own Device (BYOD) Policy**

1. **Scope:** This policy applies to all employees who work remotely or use personal devices for company business.
2. **Purpose:** To secure company data and systems accessed from remote locations or personal devices.
3. **Guidelines:**
   * Employees must use secure connections (e.g., VPN) when accessing company systems remotely.
   * Personal devices used for work must have up-to-date antivirus software and adhere to company security policies.
   * Company data must not be stored on personal devices without IT department approval.

**H. Incident Response and Reporting Policy**

1. **Scope:** This policy applies to all employees and contractors.
2. **Purpose:** To provide a structured approach to handling IT security incidents.
3. **Guidelines:**
   * Employees must report any suspected IT security incidents (e.g., phishing, malware, unauthorized access) immediately.
   * The IT department is responsible for investigating incidents and taking appropriate action.
   * Documentation of the incident, including steps taken to resolve it, must be maintained.

**IV. POLICY VIOLATION**  
Violations of this policy may result in disciplinary action, up to and including termination of employment, legal action, and/or involvement of law enforcement agencies.

**V. POLICY REVIEW**  
This policy will be reviewed annually and may be amended at the discretion of the company.

**VI. QUESTIONS**  
For any questions regarding this policy, employees should contact the IT department.

**VII. ACKNOWLEDGEMENT**  
By using the company’s IT resources, employees acknowledge that they have read, understood, and agreed to abide by this policy.