**###YOUR COMPANY NAME IT and Security Policies**

At ###YOUR COMPANY NAME, we prioritize the security and confidentiality of our data, computer systems, and network. These IT and Security Policies are in place to protect sensitive information, ensure responsible computer usage, and prevent unauthorized access to our systems. All employees are expected to comply with these policies to maintain the integrity of our IT infrastructure. Please read and adhere to the following guidelines:

**1. Acceptable Use of Technology:**

* All employees must use company-provided technology, including computers, laptops, tablets, and smartphones, responsibly and solely for work-related purposes.
* Unauthorized installation of software, apps, or hardware on company devices is strictly prohibited.
* Employees must not engage in any activities that may lead to the introduction of malware or viruses into the company's IT systems.

**2. Data Security and Confidentiality:**

* Confidential and sensitive information, such as patient records, financial data, and personal information, must be handled with the utmost care and discretion.
* Employees are responsible for safeguarding data and must not share it with unauthorized individuals or entities.
* Access to sensitive information should only be granted to employees who require it to perform their job duties.

**3. Password Protection:**

* Employees must use strong passwords for all company systems and change them regularly.
* Sharing passwords is not permitted, and each employee is responsible for maintaining the confidentiality of their login credentials.

**4. Internet Usage:**

* Internet access is provided to employees for work-related tasks only. Personal browsing should be kept to a minimum and limited to break times.
* Accessing inappropriate or unauthorized websites, downloading illegal content, or engaging in online activities that compromise the company's reputation is strictly prohibited.

**5. Email Usage:**

* Company-provided email accounts are to be used for official communication purposes only.
* Employees should exercise caution while opening emails from unknown sources and report any suspicious emails to the IT department immediately.

**6. Mobile Device Security:**

* Mobile devices provided by the company must be protected with a passcode or biometric authentication.
* In case of loss or theft of a company mobile device, employees should report it immediately to the IT department.

**7. Remote Work Security:**

* Employees working remotely must ensure they have a secure internet connection and follow the same IT and security policies as they would in the office.
* Company-provided devices should not be used by anyone other than the authorized employee.

**8. Social Engineering Awareness:**

* Employees should be cautious of social engineering attempts, such as phishing emails or phone calls, aimed at gaining access to sensitive information.
* If an employee suspects a social engineering attempt, they should report it to the IT department promptly.

Non-compliance with these IT and Security Policies may result in disciplinary action, up to and including termination of employment. By adhering to these guidelines, we can collectively maintain the security and confidentiality of our data and systems.

For any IT-related questions or concerns, please contact the IT department PHONE NUMBER or EMAIL

Thank you for your cooperation.

###YOUR COMPANY NAME