IT Policy

Email Policy

- Choose a strong password.
- Never hand out your email password to anyone.

- Don't write down your password anywhere in the notepad.
- The Company's email addresses or systems shall not be used for creating, distributing or accessing any offensive or illegal material, including but not limited to material with offensive comments about gender, race, age, sexual orientation or religious beliefs.
- Any offensive material received in the email must be reported to the IT Department and Human Resources without undue delay.
- The creation or forwarding of chain or joke letters from Company email addresses or systems is prohibited.
- The Company may monitor and record any and all email messages received or sent by email addresses or systems owned or operated by the Company. The Company does not necessarily monitor all email activity but retains the right to do so.

Acceptable Use Policy

- **Social Media:** The use of social media during work hours should be limited to business purposes. Sharing confidential information or engaging in negative discussions about the organization is prohibited.
- **Network Integrity:** Users must refrain from engaging in any activities that could negatively impact the performance, availability, or security of the organization's network.
- **Software and Hardware:** Only authorized software and hardware should be used on [Organization Name] systems. Unauthorized installation of software, hardware modifications, or attempts to bypass security measures are strictly prohibited.
- **Security:** Users are responsible for safeguarding their login credentials and ensuring that unauthorized individuals do not access the resources. Any suspicious activity should be reported immediately.
- **Data Protection:** Users are expected to respect the confidentiality, integrity, and availability of sensitive information. Data should only be accessed by authorized individuals for legitimate purposes.

- **Internet Usage:** Internet access is provided for work-related tasks. Visiting inappropriate, offensive, or potentially harmful websites is prohibited.

Remote Access Policy

- Authorized Users: Only authorized individuals with a legitimate business need are allowed remote access to [Organization Name] systems. Remote access must be approved by the relevant department or manager.

- Authentication: Multi-factor authentication (MFA) is required for all remote access connections. This adds an extra layer of security to verify the identity of the user.

- Endpoint Security: Remote devices used for accessing [Organization Name] resources must have up-to-date security software, including antivirus and anti-malware solutions. The devices should be regularly patched and updated with the latest security patches.

- Data Protection: Users are responsible for ensuring the security of data when accessed remotely. Sensitive or confidential data should not be stored on personal devices. Data should only be accessed, transmitted, and stored in accordance with organizational data protection policies.

Remote Access Methods:

- Virtual Private Network (VPN): When remote access requires network connectivity, users must connect through the organization's VPN. All traffic passing between the remote device and the organization's network should be encrypted.

BYOD Policy

- Employees are not allowed to use personal smartphones and other BYOD technology for corporate network access unless acceptance of this policy and all associated Company policies are first accepted and subsequent Company supporting security, privacy and risk technology and processes are fully implemented.

- Company Technology Resources shall not be used to download, transmit, or store objectionable material, images, or content.
- Users must not allow others to access Technology Resources by using their accounts.

- The use of third-party Technology Resources such as personal Electronic Mail or File Storage accounts outside of Company provided Technology Resources in the transmission of Company information is prohibited. Accessing third-party personal Technology Resources is only permitted while an employee is off duty and while an employee is not using Company resources. The usage of Company Technology Resources is for business purposes only.
- Jail-breaking or rooting your personally owned device is a technique that poses a risk to Company Technology Resources if it adversely impacts the intended performance of security software, data leakage controls and risk mitigating controls implemented by the Company. Disabling the technology implemented to protect Company Technology Resources can result in disciplinary actions up to and including termination of employment for employees.
- Users shall be accountable for all activity associated with their accounts.

- The Company takes no responsibility for the personal information you may have lost on your device(s) and encourages the employee to make frequent back-ups.
- When an employee leaves The Company, mobile devices owned by the user, must be wiped clean of all company data, including but not limited to corporate directory, email, applications and stored data.
- The following actions may result in disciplinary action with your supervisor and/or group manager that could result in the termination of your position within The Company:

1. Not reporting a lost or stolen device that contains customer and/or employee information (i.e., most emails) to the IT department within X hours of realizing you cannot locate your device;

2. Downloading inappropriate software on your device for the workplace;

3. Use of services/data on mobile devices in violation of corporate rules;

4. Use of services/data on mobile devices in violation of 3rd party industry standards and regulations (e.g., PCI, HIPAA, etc.);

5. Fraudulent use of devices/services;