<<Insert Logo Here>>

**Acceptable Use Policy**

***Overview***

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at \*\*\*\* in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

\*\*\*\* provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

***Scope***

All employees, contractors, consultants, temporary and other workers at \*\*\*\* including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by \*\*\*\*, or to devices that connect to a \*\*\*\* network or reside at a \*\*\*\* site.

***Policy Statement***

You are responsible for exercising good judgment regarding appropriate use of \*\*\*\* resources. \*\*\*\* resources may not be used for any unlawful or prohibited purpose.

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the \*\*\*\* network may be disconnected. Information Security prohibits actively blocking authorized audit scans.

***Passwords***

* All devices must be protected by a strong password. (See password recommendations below).
* Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends.
* Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

**Password recommendations:**

* Change passwords every 90 days or more.
* Passwords should be at least 10 characters with caps, numbers and symbols.
* Different passwords should be used for each site and never repeated.
* Never let the browser save your passwords.
* Store passwords securely. They should never be visible anywhere in your workspace.

***System Accounts***

* Always secure mobile devices. In the event of a lost or stolen mobile device it is incumbent on the user to report this to Management and alert TeamLogic IT immediately so the device can be remotely locked to prevent access.
* You must ensure that proprietary information remains within the control of \*\*\*\* at all times. Conducting \*\*\*\* business that results in the storage of proprietary information, including photographs, on personal or non- \*\*\*\* controlled environments is prohibited. This specifically prohibits the use of an e-mail account that is not provided by \*\*\*\*, or its customer and partners, for company business.

***Network Use***

You are responsible for the security and appropriate use of \*\*\*\* network resources under your control. Using \*\*\*\* resources for the following is strictly prohibited:

* Causing a security breach to either \*\*\*\* or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.
* Causing a disruption of service to network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
* Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

***USB Flash Drive Security***

SB flash drives or thumb drives pose a severe security risk to networks and data. They can be used to transmit viruses and other malware every time they are plugged into another computer.

* Regularly audit your USB device and remove any unneeded old files.
* Keep personal and business USB drives separate.
* Do not insert a USB device into a computer you don't trust.
* When you have finished transferring sensitive data from a USB drive, be sure to delete it using a secure delete utility.

***Email***

* Never access emails from public WiFi

Public WiFi is never secure, and there are many ways in which hackers can steal all the information that passes through a network. If you are unable to connect to a securely it is best to use your smartphone and mobile as an internet Hot Spot.

* Never click the “unsubscribe” link in spam emails

If you receive a suspicious email and there is an unsubscribe link at the bottom of the page, make sure you never click it. Hackers will often place them in emails in an attempt to fool you. Once you click and open the door, they are in.

* Be on the lookout for Phishing Scams

***Enforcement***

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination

of employment.

I acknowledge receipt of the acceptable use policy and agrees to comply to the standards contained in the policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date