**<Company Name> Acceptable Use Policy**

**1. Overview**

<Company Name> Acceptable Use policy seeks to protect the productivity, integrity, and security of the company. Users and customers are expected to use the company network responsibly and follow the guidelines as mentioned below.

Computer-related systems, including and not limited to network equipment, electronic mail services, and operating systems, are property of the <Company Name> company. Thus, use of said systems must serve the interests of the company and the customers it serves. It is the responsibility of each user to familiarize themselves with these policies, avoiding activities that would place the company’s welfare at risk.

**2. Purpose**

The purpose of this policy is to outline the acceptable use of organizational equipment at <Company Name>. These rules are in place to protect <Company Name> and its employees. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

**3. Scope**

This policy applies to all employees, contractors, consultants, temporaries, and other workers that interact with computing resources owned, managed, or leased by <Company Name>. All employees, contractors, consultants, temporary, and other workers at <Company Name> and its subsidiaries are responsible for exercising good judgement regarding appropriate use of information, electronic devices, and network resources in accordance with <Company Name> policies and standards, and local laws and regulations.

**4. Policy**

4.1. General Use and Ownership

4.1.1. <Company Name> proprietary information stored on company electronic and computing devices remains the sole property of <Company Name>, including both owned or leased computing devices. You must ensure that this information is protected in accordance with the Data Protection Standard.

4.1.2. <Company Name> data and intellectual property must not be stored on personal devices without prior authorization. This includes email.

4.1.3. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of <Company Name> proprietary information.

4.1.4. You may access, use or share <Company Name> proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.2. Security and Proprietary Information

4.2.1. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.2. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.3. Postings by employees from a <Company Name> email address to newsgroups should contain a disclaimer stating that the opinion expressed are strictly their own and not necessarily those of <Company Name>, unless posting is in the course of business duties.

4.2.4. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3. Unacceptable Use The following activities are prohibited. Employees may be exempted from these restriction from either authorized requests or if it concerns their legitimate job responsibilities.

<Company Name> employees are unauthorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name> owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1. Email Usage and Access

4.3.1.1. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).  
4.3.1.2. Any form of harassment via email, whether through language, frequency, or size of messages. 4.3.1.3. Unauthorized use, or forging of email header information.  
 4.3.1.4. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or collect replies.  
4.3.1.5. Creating or forwarding “chain letters”, “Ponzi”, or other “pyramid” schemes of any type.  
4.3.1.6. Use of unsolicited email originating from with the <Company Name> networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>’s Network.   
4.3.1.7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.2. Internet Usage

4.3.2.1. Employees are expected to use the Internet responsibly and productively.  
4.3.2.2. Internet access is limited to job-related activities only.  
4.3.2.3. Employees may not use the Internet for personal use that is detrimental to best interests and interferes with an employee’s regular work duties.

4.3.3. Social Media

4.3.3.1. All forms of social media are not permitted while using <Company Name>’s property and systems.

4.3.3.2. All employees are prohibited from revealing any <Company Name> confidential or proprietary information, trade secrets or any other material.

4.3.4. Storing Company Data and Intellectual Property

4.3.4.1. You must not store company data and intellectual property on personal devices without prior authorization.

4.4 USB

4.4.1. No personal USB devices are to be inserted into any company devices

4.4.2. The only USB devices to be inserted into any device are those provided by the company

4.5 Cell Phones

4.5.1. Internet and email use policies extend to the use of cell phones

4.5.2. Cell phones can be used for communication primarily for business uses

4.5.3. Cell phones can not be used for recreational purposes during work times

4.6 Cryptocurrency

4.6.1. No company devices or internet access may be used for the storage, transfer, or mining of any cryptocurrencies

4.6.2. Any cryptocurrency found on any device will be confiscated and will become property of the <Company Name> company.

4.6.2. No company resources, including but not limited to: electricity, cooling, and hardware are to be used for the storage, transfer, or mining of any cryptocurrencies

**5. Policy Compliance**

5.1 Compliance Measurement The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions Any exception to the policy must be approved by the IT team in advance.

5.3 Non-Compliance An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Peer to Peer

6.1 Peer to Peer sharing must be authorized by network.