**Internet Use Policy**

**Policy brief & purpose**

Our employee internet usage policy outlines our guidelines for using our company’s internet connection, network and equipment. We want to avoid internet use that creates risks for our company’s legality and reputation.

**Scope and Applicability**

This policy applies to all employees, contractors, and other associates of our company. By signing this document, you agree to abide by the principles stated within the policy. Violation of this policy could result in disciplinary and/or legal action including termination of your employment with our company. Employees may also be held liable for damages caused by any violations of this policy.

**Guidelines for use of the internet in the workplace**

**1.** **Restrict actions/Suggestions:**

Employees of our company are trusted to use company property in a way that is respectful and appropriate. our company has zero tolerance for comments and actions that would be considered racist, sexist, derogatory, vulgar, threatening, harassing, or otherwise discriminatory. This includes but is not limited to actions and comments partaken when using the internet and other technology provided by our company.

**2. Personal use of the internet during work hours**

Employees are expected to use company-provided internet and other devices as a resource for completing their assigned duties and supporting the objectives of our company.

Excessive personal use of company internet (“cyberloafing”) during work hours is not permitted, however occasional and reasonable personal use is acceptable, so long as:

• Frivolous use of the internet does not interfere with employee productivity, including the quality of work produced and other indicators of performance.

• The employee’s personal use of the internet does not violate any other guidelines contained within this document.

• Personal use does not cause undue effects to the company network by consuming an excessive amount of the limited available bandwidth. Examples include but are not limited to downloading/uploading unreasonably large files and streaming videos.

• Employees do not use company property to perform commercial services outside of tasks and projects assigned by our company.

3. **The following activities are strictly forbidden on company equipment:**

• Illegally downloading music, films, software, and other digital goods (“Piracy”)

• Installing software on company computers without the authorization of a company information technology (IT) representative.

• Sharing confidential material, trade secrets, or other proprietary information outside of authorized parties of our company.

• Gaining unauthorized access to programs, systems, websites, etc. (“Hacking”).

• Introducing malicious software (“Malware”) onto the company network or performing other actions that put the security of the organization at risk

• Attempting to bypass the company web filter to access blocked material.

• Accessing content that would reasonably be considered not safe for work such as pornography, violent imagery, and other adult-oriented content.

• Sharing or leaking passwords or other credentials that are used to provide access to company equipment, services, accounts, and other company assets.

**Company-issued equipment**

We expect our employees to respect and protect our company’s equipment. “Company equipment” in this computer usage policy for employees includes company-issued phones, laptops, tablets and any other electronic equipment, and belongs to our company.

We advise our employees to lock their devices in their desks when they’re not using them. Our employees are responsible for their equipment whenever they take it out of their offices.

**Email**

Our employees can use their corporate email accounts for both work-related and personal purposes as long as they don’t violate this policy’s rules. Employees shouldn’t use their corporate email to:

• Register to illegal, unsafe, disreputable or suspect websites and services.

• Send obscene, offensive or discriminatory messages and content.

• Send unauthorized advertisements or solicitation emails.

• Sign up for a competitor’s services unless authorized.

Our company has the right to monitor corporate emails. We also have the right to monitor websites employees visit on our computers.

**Disciplinary Action**

Employees who don’t conform to this employee internet usage policy will face disciplinary action. Serious violations will be cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

• Using our internet connection to steal or engage in other illegal activities.

• Causing our computers to be infected by viruses, worms or other malicious software.

• Sending offensive or inappropriate emails to our customers, colleagues or partners.

**Contact Us:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Company Name)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Company Mobile Number)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Company Email ID)