## Ports Petroleum Company, Inc.

# Electronic Device and Internet Usage Policy
# For Transport, DEF & Tank wagon Drivers

**Purpose**
The purpose of this policy is to set forth the Company Electronic Device & Internet Usage Policy by which all Transport, DEF and Tank wagon drivers will abide. The intention of this policy is to provide proper guidance to the Company drivers who make use of electronic devices and/or internet connectivity during the course of their employment with Ports Petroleum Co., Inc. As a Company driver of Ports Petroleum Co., Inc. you are required to comply with this policy at all times.

All Company drivers are required to read and sign the Electronic Device and Internet Usage Policy. A copy of this policy may be obtained from your Manager.

**Definitions**
Authorized Use - Authorized Use shall mean any use of wireless network access points or hot spots, which are deemed to be necessary and consistent with the execution of the individual duties and obligations of driver's employed by the Company.

Authorized Users - Authorized Users shall mean all current employees who are authorized by the Company to use specific network or computing resource by the department responsible for overseeing or managing the resource.

Electronic Device - Is defined as, but not limited to, hand held computing devices, laptops, tablets, desktop computers, phones or smartphones.

Internet Usage – Is defined as connectivity through wire land networks, wireless networks, cellular networks, Wi-Fi, Bluetooth or other Internet Access Points including Company internet access; its private network; its vendor suppliers and partner networks and its email system or any other access point, connection resource or broadcast which offers access to the internet.

Non Authorized Users - Non authorized Users shall mean anyone including, but not limited to, employees, contractors, vendors, or anyone else who are NOT authorized by the Company to use specific network or computing resource by the department responsible for overseeing or managing the resource.

Untrusted Networks - Untrusted Networks shall mean an insecure Public or Private Network or Internet Hotspot which offers access to the Internet and which does not employ SSL or secure encryption.

**Use of Electronic Devices and Internet**
The Company makes available its various assets, hardware, software services and computer networks in order to allow its Company driver's access to resources to effectively execute their job functions and duties.

Users are expected to use electronic equipment responsibly and professionally and shall make no use of the equipment or internet services in an illegal, malicious or obscene manner.

All Mobile Devices provided to Company drivers shall be subject to on demand audits by the IT Department or Managers to ensure compliance with this Policy.

The Company reserves the right to add, modify or delete any provision of this Agreement at any time and without notice. The Company reserves the right to restrict any access right at any time whether violation of this Policy occurs or not. The Company reserves the exclusive right and will be the sole arbiter as to what constitutes violation of any of these provisions.

All Electronic Devices provided to Company drivers may not be used for commercial or other activities from which they directly or indirectly personally profit or have profit motive.

Unacceptable use shall be defined as, but not limited to, the following examples.

- Making or receiving personal phone calls.
- Using the Internet for personal or commercial purposes.
- Sending or receiving personal email.
- Using the camera or other features on the electronic device for non-work related activities.
- Accessing pre-installed Apps, software or games for non-work related activities.
- Storing non-work related information on the electronic device.
- Downloading Shareware, Freeware programs, Apps or software that have not been authorized such as games, weather programs, driving direction programs, music apps, etc.
- Accessing Social or Professional Networking Sites such as MySpace, Facebook, Twitter, LinkedIn, Google+, Instagram, etc.
- Blogging Platforms, Blogger, BlogSpot, Word Press, Tumblr, E-Bay, Amazon, Craigslist, etc. or other sites that are non-essential to the performance of your job duties and obligations.
- Engaging in online gaming or gambling.
- Sending bulk unsolicited email Spam.
- Engaging in file sharing or Peer to Peer Networking P2P.
- Disseminating any confidential information about the Company or its customers.
- Installing ANY software on a Company computer, smart phone or other asset without prior approval from the employee's manager or IT manager.
- Compromising the security of the Company network, company computers or any other company resource by engaging in unacceptable usage of the Internet.

- Viewing, sharing or knowingly causing someone to view content that may be deemed as obscene, immoral or illegal or that may cause the Company to be held liable for discrimination or obscenity.
- Causing disruption or interference with any network or user whether associated with the Company or not.
- Searching for, requesting, acquiring, storing or disseminating images, text or data that are pornographic, whether legal or not, or that negatively depict race, religion, sex, age, or creed.
- Conducting third party business or personal business enterprise not benefiting the Company, participating in political or religious activity, engaging in illegal or fraudulent activities, or knowingly disseminating false or otherwise libelous materials.
- Accessing any Company resource or asset that is not within the scope of the user's normal work and job functions. Examples include, but are not limited to, customer information, personnel files and data or any other documents not required for the proper execution of the user's normal job functions or duties.
- Any other illegal purpose, listed here or not, through an internet network or not, that would encourage or conduct criminal activity offense, exposure to civil liability or otherwise violate any local, state, federal or international law.

The following will also be construed as violations.

- Allowing access to any restricted information by individuals or allowing individuals to gain access to Electronic Devices for non-company or non-authorized activities.
- Allowing any software or application to be installed on the Electronic Device at any time.
- Engaging in any behavior with the Electronic Device that would violate the Company Electronic Device and Internet Usage Policy.

**Inappropriate Use of Resources**

Inappropriate use of resources shall be defined as engaging in any activities by users that are inconsistent with the business needs and goals of the Company. Engaging in any activity that adversely affects the user's productivity will not be tolerated. When you access the Internet for business purposes you are representing the Company with each site or activity you engage in. Special attention must be paid to such activities that do not directly contribute to the fulfillment of the employee's job description or duties.

**Responsibility for Online Activities**

Users are responsible for their online activities. Each employee must indemnify Ports Petroleum Co., Inc. from all claims of loss whether direct or indirect and from any consequential losses suffered by the Company due to breach of the Company Electronic Device and Internet Usage Policy. Ports Petroleum Co., Inc. is not responsible for users who display, store or otherwise transmit any personal information such as passwords, banking information, credit card numbers, social security, or tax ID numbers or make use of Internet passports or wallets.

Ports Petroleum Co., Inc. shall not be held liable for damages resulting from any loss of such information abuse by other parties or any consequential loss of personal property or injury resulting from the storage or loss of such information.

**Sensitive and Confidential Information**
Every employee has the obligation to protect sensitive and confidential information.

**Consequences of Violations**
Failure to adhere to the policies and provisions of this Policy may result in disciplinary actions up to and including termination.

**Improper or Illegal Conduct**
Ports Petroleum Co., Inc. also reserves the right to pursue legal remedy for damages incurred as a result of an employee's violation. Certain illegal activities will require the Company to immediately notify or comply with the proper authorities upon discovery. The Company reserves the right to examine any user's Email Account, Web Logs, Chat Logs, Phone Numbers or any other information passed through Company resources or Networks or stored on Company computers or cell phones at any time and without prior notice.

**Effective Date**
The practices described in this Wireless Network Usage Policy are current as of **Sept. 04, 2012**.

Use of any company electronic equipment or accessing company network resource or Internet Access Point implies an agreement to abide by all Company policies and procedures.

I hereby declare that I have read and fully understand my duties and obligations set forth in the above Electronic Device & Internet Usage Policy for Ports Petroleum Company, Inc. and will uphold these duties and obligations at all times.

Employee Name: _____

Employee Signature: _____

Date: _____