**BACKCOUNTRY ACCEPTABLE USE POLICY**

**PURPOSE**

Establish acceptable and unacceptable use of Internet resources as email, remote access and wireless technologies, laptops, tablets, removable electronic media, and email usage.

This acceptable usage policy covers the security and provides the guidelines about the appropriate use of Internet access.

Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner.

**SCOPE**

The Acceptable Use Policy applies to all employees who have access to computers to be use in the performance of their work, and the devices that connect a network or interact with internal networks and business systems, including all services provided with the TCP/IP protocol, remote access and wireless technologies, electronic mail (e-mail), file transfer protocol (FTP) and World Wide Web access.

The Acceptable/Unacceptable Use Policies applies to all devices that need to connect with the internal Company network and also covers all IT information communications facilities operated by BackCountry. Have a policy in place helps to protect both the business and the employee and promote the integrity and security of the systems and network.

**AUDIENCE**

This acceptable use policy is intended for and should be distributed to all BackCountry personnel and vendors who have access to the internal network. It must be reviewed and/or updated as needed, and at least annually, to reflect changes to business objectives or the risk environment. Changes to the policy must be communicated to all relevant personnel.

**POLICY**

**1: General Internet Acceptable Use**

Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role.

Company employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted

The Internet access is permitted by employees where use supports the goals and objectives of the business performing their jobs. Personal use is permitted where such use does not affect the individual’s business performance.

BackCountry provides computers and Internet connections to further its business interests; the company has the right to monitor all Internet searches, communications and downloads that pass through its facilities.

The employees must sure that they:

* Use the Internet in a acceptable way.
* Comply with current legislation.
* Avoid business risk by their misuse of the Internet.

Employees need to be warned about the dangers that downloading unknown files can present, download attachments or software onto a work computer increases the risk of a virus infection throughout the network.

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

All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

**2: General Internet Unacceptable Use**

The following activities are in general prohibited:

Using computers to perpetrate any form of fraud, and/or software, film or music piracy.

Stealing, using, or disclosing someone else's password without authorization.

Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.

Sharing confidential material, trade secrets, or proprietary information outside of the organization.

Introducing malicious software onto the company network.

Spending more than 30 minutes of the working day looking at non-business related Internet sites.

**3: Email and Communication Unacceptable Use**

When using Company resources to access and use the Internet, employees must realize they represent the company. BackCountry personnel must be aware to avoid the following unacceptable practices:

Sending unsolicited email message, including the sending of “junk mail” or other advertising material that did not specifically request.

Any form of harassment via email.

Unauthorized use, of email header information.

Using email for personal, non-business related communication during working hours.

Sending e-mails, either internally or externally, saving or storing attachments or documents which could be regarded as:

Harassment, victimization or bullying

Discriminatory

Abusive

Pornographic

Obscene

Illegal

Offensive

Abuse of ABC Company’s logo or Company name

**4: Email and Communication Acceptable Use**

Occasional personal use.

Be careful when sending emails containing personal or confidential information. Check the recipient’s name, especially if there is more than one person with the same name.

The receipt of any email communication containing obscene material must be reported immediately

**5: Working off-site Acceptable**

Working away from the offices must be in line with remote working policy.

Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.

Laptops must be carried as hand luggage when travelling.

Information should be protected against loss or compromise when working remotely.

Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

**6: VPN Service**

Employees, and authorized third parties may, utilize remote access to access BackCountry computing resources.

All computers connected to BackCountry via VPN should be configured with up to date anti-virus, operating system updates, and active firewall software.

Periodic audits of VPN access for verify that the actual user connected to the VPN no have any problems, and their account has not been compromised.

Secure remote access must be strictly controlled.