

# Acceptable Use Policy

## Introduction

This Acceptable Use Policy (the "Policy" or "AUP") outlines the terms and conditions for using Gridley Communications, Inc. d/b/a Gridcom ("Gridcom") Services. By accessing and using our Services, you agree to abide by this Policy. Services must be used in a manner that is consistent with the intended purpose of the Services and Gridcom's Terms and Conditions. If you do not agree with any part of this Policy, you should refrain from using the Services.

**By using Gridcom's Service(s), you, Customer, agree to comply with this Acceptable Use Policy and to remain responsible for your use and the use of any Customers under your control.**

## Purpose of this Policy

The purpose of this Policy is to ensure a safe, respectful, and lawful online environment for all Customers of the Services. This Policy governs the use of the Services, including all content, features, and usage of the Services.

The Service may only be used for lawful purposes for your individual use. You agree to use responsible Internet practices, including, without limitation, using computer security and anti-virus protections, to ensure that unauthorized third parties do not gain access to your computer or computer network or the Service.

## Prohibited Activities

### General Prohibitions:

Gridcom prohibits the use of the Services in any way that is unlawful, harmful to, or interferes with the use of Gridcom's network or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening or offensive material, or constitutes SPAM/E-mail/Internet abuse, a security risk or a violation of privacy.

### Unlawful Activities:

Services shall not be used in connection with any criminal, civil, or administrative violation of any applicable local, state, provincial, federal, national, or international law, treaty, court order, ordinance, regulation, or administrative rule.

### Violation of Intellectual Property Rights:

IP Service(s) shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property

rights or privacy or publicity rights of Gridcom or any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

## Threatening Material or Content:

Services shall not be used to host, post, transmit, or re-transmit any content or material (or to create a domain name or operate from a domain name) that harasses or threatens the health or safety of others. In addition, for those Services that utilize Gridcom-provided web hosting, Gridcom reserves the right to decline to provide Services if the content is determined by Gridcom to be obscene, indecent, hateful, malicious, racist, defamatory, fraudulent, libelous, treasonous, excessively violent, or promoting the use of violence or otherwise harmful to others.

## Customer Responsibilities

Customers are responsible for any use or misuse of the Service that violates this AUP, even if it was committed by a friend, family member, or guest with access to your Service account. This includes responsibility for the content of any material posted, hosted, downloaded/uploaded, created, accessed, or transmitted using the Services.

Customers are also solely responsible for the security of any device connected to the Service, including any data stored or shared on that device. It is the Customer's responsibility to secure the Customer's equipment and any other premises equipment or programs not provided by Gridcom that connect to the Service from external threats such as viruses, spam, botnets, and other methods of intrusion.

Gridcom takes no responsibility for any material created or accessible on or through the Services and will not exercise any editorial control over such material. Gridcom is not obligated to monitor the Services but reserves the right to do so.

## Security Violations

Customers are responsible for ensuring and maintaining the security of their systems and the machines that connect to and use Service(s), including implementation of necessary patches and operating system updates.

Services may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of Gridcom's (or another party's) server, network, network access, personal computer or control devices, software or data, or other system, or to attempt to do any of the foregoing.

Examples of system or network security violations include but are not limited to:

- unauthorized monitoring, scanning, or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of e-mail addresses;
- hacking, attacking, gaining access to, breaching, circumventing, or testing the vulnerability of the user authentication or security of any host, network, server, personal computer,

network access, and control devices, software, or data without express authorization of the owner of the system or network;

- impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
- using any program, file, script, command, or transmission of any message or content of any kind designed to interfere with a terminal session, the access to or use of the Internet, or any other means of communication;
- knowingly uploading or distributing files that contain viruses, spyware, Trojan horses, worms, time bombs, cancelbots, corrupted files, rootkits, or any other similar software or programs that may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hi-jacking;
- engaging in the transmission of pirated software or violating intellectual property laws;
- providing guidance, information, or assistance with respect to causing damage or security breach to Gridcom's network or systems or to the network of any other IP Service provider.

## Spam/E-mail/Usenet Abuse:

Violation of the CAN-SPAM Act of 2003, or any other applicable law regulating e-mail services, constitutes a violation of this AUP. SPAM/E-mail abuse is prohibited using Services. Examples of SPAM/E-mail abuse include but are not limited to the following activities:

- sending multiple unsolicited electronic mail messages or "mail-bombing" – to one or more recipient;
- sending unsolicited commercial e-mail or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;
- sending unsolicited electronic messages with petitions for signatures or requests for charitable donations or sending any chain mail-related materials;
- sending electronic messages, files, or other transmissions that exceed contracted capacity or that create the potential for disruption of the company's network or of the networks with which the company interconnects by virtue of quantity, size, or otherwise;
- using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients as to the origin or to conduct any of the activities prohibited by this AUP;
- using IP addresses that the Customer does not have a right to use;
- sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the Services or the Internet (e.g., through language, frequency, size, or otherwise);
- using distribution lists containing addresses that include those who have opted out;

- sending electronic messages that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header;
- falsifying packet header, sender, or user information, whether in whole or in part, to mask the identity of the sender, originator, or point of origin;
- using redirect links in unsolicited commercial e-mail to advertise a website or service;
- intercepting, redirecting, or otherwise interfering or attempting to interfere with e-mail intended for third parties;
- using, distributing, advertising, transmitting, or otherwise making available any software program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, including, but not limited to, the facilitation of the means to spam.

## Enforcement and Notice

In most cases, Gridcom will notify Customers of complaints received by Gridcom regarding an alleged violation of this Policy. You agree to promptly investigate all such complaints and take all necessary actions to remedy any violations of this Policy. Gridcom may inform the complainant that you are investigating the complaint and may provide the complainant with the necessary information to contact you directly to resolve the complaint.

Gridcom nevertheless reserves the right to take down any material—or otherwise block access to—created or accessible on or through the Services and suspend or terminate any user creating, storing, or disseminating such material where Gridcom becomes aware that the material violates this AUP and/or exposes Gridcom to civil or criminal liability, including without limitation, under applicable copyright laws. Gridcom reserves the right to avail itself of the safe harbor provisions of the [Digital Millennium Copyright Act \[LINK TO POLICY\]](#).

Gridcom reserves the right to act immediately and without notice to suspend or terminate affected Services in response to a court order or government notice that certain conduct must be stopped or when Gridcom reasonably determines that the Customer's use of the affected Services may: (1) expose Gridcom to sanctions, prosecution, civil action or any other liability; (2) cause harm to or interfere with the integrity or normal operations of Gridcom's network or networks with which Gridcom is interconnected; (3) interfere with another Gridcom Customer's use of Services or the Internet; (4) violate any applicable law, rule or regulation; or (5) otherwise present an imminent risk of harm to Gridcom or Gridcom Customers.

Gridcom shall cooperate with legal authorities and third parties in the investigation of any alleged wrongdoing related to this AUP, including disclosing the identity of the user that Gridcom deems responsible for the wrongdoing. Gridcom will not be liable for any damages of any nature suffered by any user or any third party resulting in whole or in part from Gridcom's exercise of its rights under this AUP.

## Updates to this AUP

Gridcom reserves the right to change or modify the terms of the AUP at any time. Changes shall become effective when posted on Gridcom's website and continued use of the Services after updates shall constitute acceptance of any new or updated terms.