

Pelion Connectivity Management
Acceptable Use Policy

1. Customer is responsible for any transmission sent, received, posted, accessed, or stored via the Customer Solution, including the content of any communication. Transmitting, distributing, or storing any material or using the Service in a manner that breaches any applicable law is prohibited. Without limiting the generality of the foregoing, Customer shall not, and shall ensure that the Customer End Users shall not use the Customer Solution (or any part thereof):
 - (a) to send, disseminate or post any material or communications which are libelous, defamatory, offensive, indecent, lewd, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, menacing, inflammatory, obscene, annoying, incite hatred, panic or anxiety or which are otherwise objectionable or unlawful;
 - (b) to access, transmit, publish, display, advertise or make available material which infringes copyright or any other intellectual property right held in any country, is obscene or pornographic, contains threats of any kind, is defamatory in any way or breaches confidence, which is illegal or infringes any third party's legal rights of whatsoever nature under the laws of any jurisdiction for any reason;
 - (c) in a manner which consumes disproportionate (depending on the specific state of the network at any given time) or excessive amount of available network resources (as compared to a typical user of the Customer Solution) resulting in the potential to disrupt or degrade the network or Customer Solution or network usage by others;
 - (d) to continually or repeatedly dial telephone numbers associated with free conference calls, free chat lines, or similar or related services;
 - (e) to conduct fraudulent business operations and practices, offer or disseminate fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, chain letters, and pyramid schemes); or to represent itself as an authorized 3rd party affiliate or agent for a business entity (e.g., Arm) without the business' prior consent;
 - (f) to impersonate any person or entity; falsely state or otherwise misrepresent its affiliation with any person or entity; or create a false identity for the purpose of misleading others (including using invalid or forged headers, invalid or non-existent domain names, or other means of deceptive addressing);
 - (g) in breach of the rules, regulations, or policies that apply to any third-party network, server, computer database, or website that Customer or Customer End Users access;
 - (h) to disseminate or post content that is harmful to the Customer Solution or other users of the Customer Solution including, without limitation, viruses, Trojan horses, worms, time bombs, zombies, cancelbots, or any other computer programming routines that may damage, interfere with, secretly intercept or seize any system, program, data, or personal information; or
 - (i) so as to conflict with any accepted industry guidelines, practices, codes or memoranda of understanding.
2. Customer shall not, and will ensure Customer End Users shall not, distribute, publish, or send through the Customer Solution:
 - (a) any spam, including any unsolicited advertisements, solicitations, commercial e-mail messages, informational announcements, or promotional messages of any kind;
 - (b) chain mail;
 - (c) numerous copies of the same or substantially similar messages;
 - (d) empty messages or messages that contain no substantive content;
 - (e) very large messages or files that disrupt a server, account, newsgroup, or chat service; or
 - (f) any message that is categorized as "phishing."
3. Customer shall not, and will ensure Customer End Users shall not:
 - (a) participate in spidering, harvesting, or any other unauthorized collection of e-mail addresses, screen names, or other identifiers of others or participate in using software (including "spyware") designed to

- facilitate such activity;
- (b) collect responses from unsolicited messages; or
 - (c) use any of Arm mail servers or another site's mail server to relay mail without the express permission of the account holder or the site.
4. Customer shall not, and will ensure Customer End Users shall not, breach the security of the Customer Solution in any way. Without limiting the generality of the foregoing, Customer shall not, and will ensure Customer End Users shall not, engage in any of the following activities:
- (a) unauthorized access to or use of data, systems, or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without the express prior authorization of the owner of the system or network;
 - (b) unauthorized monitoring of data or traffic on any network or system without the express prior authorization of the owner of the system or network;
 - (c) interference with service to any user, host, or network including, without limitation, denial-of-service attacks, mail bombing, news bombing, other flooding techniques, deliberate attempts to overload a system, and broadcast attacks;
 - (d) using, selling, or distributing any computer program designed to conceal the source or routing information of electronic mail messages in a manner that falsifies an Internet domain, header information, date or time stamp, originating e-mail address, or other identifier.
 - (e) using manual or electronic means to avoid any limitations established by Arm or attempting to gain unauthorized access to, alter, or destroy any information that relates to any Arm customer or other end-user.
5. Arm may, but is not obligated to, take any action it deems necessary to (1) protect the Customer Solution, its rights, or the rights of its customers or third parties, (2) optimize or improve the Customer Solution or its other Customer Solution, systems, and equipment, or (3) to protect against any wrongdoing related to or violations of this AUP. Customer acknowledges that such action may include, without limitation, suspending or terminating the Service, monitoring or restricting uses of the Service, or employing methods, technologies, or procedures to filter or block messages sent through the Customer Solution. Arm may, in its sole discretion and at any time, filter "spam" or prevent "hacking," "viruses," or other potential harms without regard to any preference Customer may have communicated to Arm.
6. Arm also reserves the right to cooperate with legal authorities and third parties in the investigation of any alleged wrongdoing related to this AUP, including the disclosure of the identity of the User that Arm deems responsible for the wrongdoing.
7. Arm will not be liable for any damages of any nature suffered by Customer, Customer End User, or any third party resulting in whole or in part from Arm's exercise of its rights under this AUP. Customer is solely responsible for all content that it transmits or receives utilizing the Customer Solution, and Customer is responsible for abuse of its account by others.