**RedEye Network Solutions, LLC**

**Customer Acceptable Use Policy (“AUP”)**

**(https://redeyenetworks.com/aup)**

The AUP or (“Policy”) defines the behaviors that are not acceptable by users, RedEye Customers or other external parties (“You” or “Your”) that are used to host RedEye Network Solutions (“RedEye”, “We”, or “Our”) products and services or providing services (collectively, the “Services”) that can include, but are not limited to, the company website (<http://redeyenetworks.com>), network, hardware, software, licenses, and other services established by RedEye, its partners, and affiliates used to engage, connect to, and/or deliver services to its customers. You may access and use RedEye Services for lawful purposes and in the manner intended for the Services, and per the terms of Your relevant agreement.

**Security and Network Integrity**

You may not use the Services to violate the security or integrity of any network, communications system, software application, or network or computing device (each a “System” or collectively, the “Systems”). The following is not an exhaustive list but provides examples of activities that are prohibited:

* Flooding a System with communication requests so that the System either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.
* Forging TCPIP packet headers, e-mail headers, or any part of a message describing its origin or route or attempting to impersonate any of Our employees or representatives.
* Interfering with the functioning of any System, including any attempt whether deliberate or not to overload a system or interfering with Our ability to deliver normal operations.
* Accessing or using any System without Our permission.
* Monitoring data or traffic on a System without Our permission.
* Using manual or electronic means to avoid any use limitations placed on a System, such as access or storage restrictions.
* Harvesting or scraping any content from the Services with methods such as manual or automated software, robotic process automation, devices, or other processes.
* Bypassing, circumventing, or attempting to bypass or circumvent, any security or authentication measures We may use to prevent or restrict access to Services.

**Illegal or Harmful Use**

You may not use, promote, facilitate, or instruct others to use the Services for any illegal, harmful, fraudulent, infringing, or offensive use, or to display, transmit, store, distribute, or otherwise, make available content that is illegal, harmful, fraudulent, infringing, or offensive. The following is not an exhaustive list but provides examples of illegal or harmful conduct that is prohibited:

* Content or computer technology that may damage, interfere with, covertly intercept, or disrupt Services, including Trojan horses, viruses, worms, botnets, spyware, time bombs, keystroke loggers, rootkits, and adware.
* Use of the Services to distribute, process or store pornographic material, inappropriate files, or files that might adversely or negatively reflect upon RedEye or be contrary to Our best interests.
* Infringement of intellectual property rights or other proprietary rights including without limitation, material protected by copyright, trademark, patent, trade secret or other intellectual property right. Infringement may result from the unauthorized copying, distribution, and/or posting of pictures, logos, software, articles, musical works, and videos.
* Failure to abide by the end user license agreements (EULAs) for software and hardware licenses provided by third party vendors whether purchased by RedEye or yourself and/or company that are applied to the RedEye network and/or systems.
* Collecting or using email addresses, screen names or other identifiers without the consent of the person identified (including, without limitation, business email compromise, Internet scamming, phishing, password spraying, spidering, and harvesting).
* Content that constitutes unauthorized or unsolicited advertising, junk, or bulk-email, such as spamming, or contains software viruses or other computer codes, files or programs that are designed or intended to disrupt, damage, limit, or interfere with the proper function of any software, hardware, or telecommunications equipment or to damage or obtain unauthorized access to any system, data, password, or other information belonging to RedEye or any other third party.

**Excessive Use of System Resources**

You may not use the Services in a manner that will unnecessarily interfere with the ability of RedEye to perform normal operations. In this situation, RedEye will ask you to repair abnormalities on your systems or network if determined it is the cause of such interruption of normal operations or disconnect the Services until the abnormality can be repaired.

**Vulnerability Testing**

You are not permitted to probe, scan, penetrate or test the vulnerability of a RedEye network or system or to breach RedEye’s system and network boundaries, or its security or authentication measures, whether with intrusive or passive techniques, with the express written permission of RedEye.

**Investigation and Enforcement**

RedEye reserves the right to investigate any suspected violation of the AUP. In addition, RedEye may report any activity that it believes is a violation of law or regulations, including, to assist law enforcement officials, regulators, or other appropriate third parties with the collection and sharing of information to help in such an investigation.

We may remove, disable access, or modify any content or resources that violates this Policy or Agreements RedEye has with you, and may terminate the Services and/or related Agreements with or without notice.

**Violations of This Policy**

Violations or a suspicion of violation should be reported immediately to abuse@redeyenetworks.com. You agree to provide RedEye with assistance to stop or remedy a violation as requested.