ACCEPTABLE USE POLICY AND TECHNICAL RESTRICTIONS

1. CUSTOMER OBLIGATIONS

Customer shall impose terms of service, technical restrictions and network use restrictions that will apply to each End User of the Internet Services, as provided by Panasonic. Panasonic may, in its sole discretion, block or otherwise restrict any End User from any use of the Internet Services that violates the restrictions in this **Acceptable Use Policy** or any other terms of service that apply to the Internet Services.

1.1 Terms of Acceptable Use

Before allowing End Users to access the Internet Services onboard Customer's Active Aircraft, Customer shall require each End User to agree to terms of acceptable use that include the following requirements or their substantive equivalent:

End Users must not:

(a) post, store, transmit or disseminate information, data or material that is libelous, obscene, unlawful, threatening or defamatory, or that infringes the Intellectual Property Right of any person or entity, or that constitutes or encourages conduct that would be a criminal offense, or otherwise violate any law;

(b) post, store, send, transmit, or disseminate any information or material that a person of various cultural backgrounds reasonably could find to be indecent, pornographic, harassing, threatening, hateful, or intimidating;

(c) upload, post, publish, transmit, reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the Internet Services or otherwise that is protected by another person's Intellectual Property Right, without obtaining permission of the owner or licensee of the Intellectual Property Right, unless the particular use of that material is subject to "fair use" under U.S. copyright law or any substantially similar principle of law in other jurisdictions;

(d) transmit unsolicited bulk or commercial messages commonly known as "spam;"

(e) send numerous copies of the same or substantially similar messages, empty messages, or messages which contain no substantive content, or send messages or files that are of a sufficient size to disrupt a server, account, newsgroup, or chat service;

(f) initiate, perpetuate, or in any way participate in any pyramid or other illegal scheme;

(g) **p**articipate in the collection of e-mail addresses, screen names, or other identifiers of others (without their prior consent), a practice sometimes known as spidering or harvesting, or participate in the use of software (including "spyware") designed to facilitate this activity;

(h) collect responses from unsolicited bulk messages;

(i) falsify, alter, or remove message headers;

(j) impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar fraudulent activity (for example, "phishing"); or,

(k) violate the rules, regulations, or policies that apply to any network, server, computer database, or website that is accessed.

1.2 TECHNICAL RESTRICTIONS

End Users of the Internet Services must not conduct any of the following activities:

(a) accessing any other person's computer or computer system, network, software, or data without his or her knowledge and consent;

(b) breaching the security of another End User or system;

(c) attempting to circumvent the User authentication or security of any host, network, or account;

(d) accessing another person's data;

(e) logging into or making use of another person's account or server without expressed authorization;

(f) probing the security of other hosts, networks, or accounts without expressed permission from Panasonic to do so;

(g) using or distributing tools or devices designed or used for compromising security, such as password-guessing programs, decoders, password gatherers, unauthorized keystroke loggers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan Horse programs;

(h) conducting port scanning without authorization from Panasonic;

(i) distributing programs that make unauthorized changes to software (cracks); or

(j) using or running dedicated, stand-alone equipment or servers from the Active Aircraft that provide network content or any other services to anyone outside of the Active Aircraft, also commonly referred to as public services or servers. Examples of prohibited equipment and servers include, e-mail, Web hosting file sharing, and proxy services and servers.

3.3 NETWORK USAGE RESTRICTIONS

End Users of the Internet Services must not:

(a) restrict, inhibit, or otherwise interfere with the ability of any other person to use the Internet Services, regardless of intent, purpose or knowledge, including the posting or transmitting any information or software that contains a worm, virus, or other harmful feature, or generating levels of traffic sufficient to impede others' ability to use, send, or retrieve information;

(b) restrict, inhibit, interfere with, or otherwise disrupt or cause a performance degradation, regardless of intent, purpose or knowledge, to the Internet Services or any host, server, backbone network, node or service, or otherwise cause a performance degradation to any facilities used to deliver the Internet Services;

(c) resell the Internet Services or otherwise make available to anyone outside the Active Aircraft the ability to use the Internet Services (for example, though Wi-Fi or other methods of networking), in whole or in part, directly or indirectly;

(d) interfere with computer networking or telecommunications service to any User, host or network, including denial-of-service attacks, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to "crash" a host and accessing and using the Internet Services with anything other than a dynamic Internet Protocol ("**IP**") address that adheres to the dynamic host configuration protocol "**DHCP**").

2. DHCP CONFIGURATION

Panasonic shall not configure the Internet Services or any related equipment to access or use a static IP address or use any protocol other than DHCP.

3. NETWORK MANAGEMENT

(a) Panasonic will operate and distribute its network resources in a manner that provides optimal service for all users of Panasonic connectivity services throughout the world. Customer acknowledges that Panasonic will be managing the network to provide a positive End User Connectivity Services experience and to provide Panasonic the ability to have insight into the internet traffic that traverses its network. To provide this experience, Panasonic will employ network management tools and techniques, including traffic-shaping policies ("**TSP**s"), which regulate network data transfer to assure a certain level of performance and quality of

service (“**QoS**”). TSPs will apply network traffic rules to apportion bandwidth at the User level and by App category to optimize the experience for all Users. QoS will enforce fair queueing and equitable prioritization of access to all Users in order to prevent a small minority of Users from monopolizing the available network resources that degrades the experience of the majority of Users.

(b) Panasonic will base network management and TSPs on identification and categorization of traffic. The TSPs maintain and continuously update a signature library containing correlating patterns for each part of the Services and application and assigns them to a categorization hierarchy. Panasonic will update signatures frequently to account for new or modified applications and parts of the Connectivity Services. Panasonic may rate-limit to a pre-defined metric all categories, applications and part of the Connectivity Services. Rate limits will apply per-End User device, and shaping starts at session initiation-first packet. The network transmission links and other resources that are used to provide the Connectivity Services are shared among all Panasonic customers. Panasonic will accordingly manage the network for the benefit of all users of the Connetivity Services. Panasonic will manage the traffic management definitions and updates, which may be set or changed without notice to Customer or End Users as internet trends and apps change.

(c) Panasonic may engage in reasonable network management practices and protect the network from harm, compromised capacity, degradation in performance or service levels, or uses of the Connectivity Services that may adversely impact access to or the use of the Connectivity Services by other customers. Reasonable network management practices that Panasonic may adopt include: (i) applying quota management on data usage; (ii) applying traffic ratings by time-of-day or User type; and/or, (iii) a modification of a limitation on a customer’s data throughput speed or data consumption.