ACCESS POLICY

This Access Policy (the "**Policy**") is incorporated by reference and forms part of all agreements entered into between Company and Panasonic Avionics Corporation ("**PAC**") (collectively, the "**Agreements**"). This Policy applies whenever Company or Company's Authorized Users (defined below) access PAC's information asset inventory (the "**Network**") or business premises (the "**Site**") (collectively, the "**Purpose**").

1. **Grant of Access**. PAC hereby grants Company temporary access to the Network and/or Site subject to this Policy.

2. **Authorized Users**.

(a) Only Company's Authorized Users may access the Network and/or the Site and only for the Purpose, in accordance with any applicable instructions or user guides PAC may provide and modify from time to time. As used in this Policy, "**Authorized User**" means Company's employees and contractors designated by Company and approved by PAC to access the Network and/or the Site for the Purpose.

(b) Company may request that PAC add a new user as an Authorized User, either as a replacement or an additional Authorized User, and in that event Company shall provide PAC with all information regarding the proposed new user as PAC may reasonably require. PAC may approve or disapprove any new additional or replacement user in its discretion, and no access will be provided to any new additional or replacement user unless PAC approves that access in writing. PAC will revoke access for any Authorized User so replaced. Company shall promptly notify PAC when an Authorized User leaves his/her employment or other business relationship with Company or is otherwise no longer eligible as an Authorized User.

(c) Company warrants that (i) all Authorized Users are employees of Company, or personnel contracted by Company to provide goods or services related to the Purpose; and (ii) that all Authorized Users have been made aware of this Policy and have agreed, as part of their employment and/or contract with Company, to comply with this Policy.

3. **Network Access**.

(a) Authorized Users may access and use the Network only by using security protocols that PAC specifies, which may change from time to time in PAC's sole discretion. The security protocols may include installation of the SecureConnector agent (or similar agent) on each Authorized User's device that is utilized to access the Network. The agent can be configured to dissolve on reboot; however, the agent must be installed and confirmed by PAC to be operational each time the Authorized User attempts to access the Network. PAC shall provide each Authorized User with a unique log-on identification code and a password (together, the "**Access Credentials**"). Company shall ensure that its Authorized Users will not share the Access Credentials with any other entity or individual, including other Authorized Users. Company shall maintain the Access Credentials in strict confidence and shall ensure that its Authorized Users do so. Company shall instruct each Authorized User as to the confidentiality of the Access Credentials and the restrictions on their use as provided in this Policy. Company shall take all necessary precautions to ensure that no other person, except its Authorized Users, will use the Access Credentials. Access Credentials are deemed to be Confidential Information under this Policy, and if put into writing, shall be stored in a secure manner, with at least the same degree of care that Company uses to protect its own confidential or proprietary information, to reasonably prevent unauthorized use of the Network and/or Site. Any failure to comply with this Section 3(a) will be a material breach of this Policy.

(b) Company shall not: (i) send or store viruses, worms, time bombs, Trojan horses and other malicious code, files, scripts, agents or programs to or in the Network; (ii) interfere with or disrupt performance of the Network or the data contained in the Network; (iii) attempt to gain access to the Network or its related systems or networks in a manner contrary to PAC's instructions; (iv) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share, offer in a service bureau, or otherwise make the Network available to any non-party, other than to Authorized Users as this Policy permits; (v) copy any features, functions, integrations, interfaces or graphics of the Network; or (vi) use the Network for any illegal purposes or activities.

(c) Company shall: (a) immediately notify Panasonic of any unauthorized use of any Access Credentials or any other known or suspected breach of security with respect to the Network; (b) immediately report to Panasonic and use reasonable efforts to stop immediately any known copying or distribution of the Networks' content; and (c) not impersonate a Panasonic user or provide false identity information to gain access to or use the Network.

4. Site Access.

(a) Authorized Users may access and use the Site only by using security protocols that PAC specifies, which may change from time to time in PAC's sole discretion. Authorized Users must: (i) provide appropriate picture identification, (ii) obtain a visitor badge, (iii) wear the badge in a visible location on the visitor's person, (iv) be escorted by a PAC employee on Site (with the exception for those who have obtained a long-term visitor pass), and (v) return the visitor badge to PAC upon leaving the Site.

(b) Company shall not: (i) interfere with or disrupt PAC's access and use of the Site; (ii) attempt to gain access to the Site in a manner contrary to PAC's instructions; (iii) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share, offer in a service bureau, or otherwise make the Site available to any third party, other than to Authorized Users as permitted herein; (iv) modify, destroy, or remove from the Site any data, documents, equipment, or other materials located in the Site without the express written consent of PAC; or (v) use the Site for any illegal purposes or activities.

5. Company's Responsibilities/Use of the Network.

(a) Company shall comply with all PAC policies concerning the security of the Network and of the Site. While accessing the Network and/or the Site, Company shall comply with PAC's Equal Employment Opportunity Statement & Policy on Prevention of Harassment, Discrimination, and Retaliation (available at https://www.panasonic.aero/public-policy/). Company will be responsible for all Authorized Users' access and use of the Network and the Site and compliance with this Policy. Company shall promptly notify PAC of any unauthorized access or use that comes to its attention.

(b) Company will be responsible for all uses of Network that result from access that Company provides, whether or not this Policy permits those uses. Company will be responsible for all acts and omissions of Authorized Users, and an Authorized User's act or omission that would constitute a breach of this Policy if Company had been responsible for the act or omission will be deemed a breach of this Policy by Company. Company shall use reasonable efforts to make all Authorized Users aware of this Policy's requirements that apply to Authorized Users' use of the Network and shall require Authorized Users to comply with these requirements.

6. Use Restrictions. The Network and its content constitutes protected copyrighted material and valuable trade secrets of Panasonic. Company shall not, and shall not permit any other person, including Authorized Users, to:

(a) copy, modify, or create derivative works or improvements of the Network or its content;

(b) use the content in any analytics tool or reorder the content or represent the content in any way for any purpose;

(c) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, commercially exploit, or otherwise make available the Network or its content;

(d) create internet links to the Network or frame or mirror any content on any other server or device;

(e) copy any of the Network's features, functions, or graphics

(f) reverse-engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to any software component of the Network, in whole or in part;

(f) remove any proprietary notices from the Network;

(g) perform or disclose any benchmarking or performance testing data of the Network;

(h) disclose the Network, including any underlying data or content, without Panasonic's explicit, written consent;

(i) use the Network for any purpose that violates any Intellectual Property Right, or that otherwise violates any law or regulation, or that is not otherwise provided for under this Policy

7. Suspension. Panasonic may temporarily suspend any Authorized Users access to the Network if:

(a) Panasonic reasonably determines that there is a threatened or actual attack on any part of the Network;

(b) Company's or any Authorized User's use of the Network disrupts or poses an identifiable security risk;

(c) Company, or any Authorized User, uses the Network in connection with any fraudulent or illegal activity, including the violation of any non-party's or Panasonic's Intellectual Property Rights;

(d) Company or any Authorized User uses the Network to send or store infringing, obscene, threatening, defamatory, or material that violates any non-party's privacy rights;

(e) Company or any Authorized User uses the Network to send or store material that contains software viruses, worms, Trojan horses, or other harmful computer code;

(f) Company or any Authorized User attempts to gain unauthorized access to the Network or its related systems or networks;

(g) Company has ceased doing business, made an assignment for the benefit of creditors or similar disposition of its assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution, or similar proceeding;

(h) Company or any Authorized User has violated the use restrictions listed in **Section 6** of this Policy;

(i) the law prohibits Panasonic's provision of the Network to Company or any Authorized User; or

(j) one or more Panasonic suppliers have suspended or terminated Panasonic's access to or use of any non-party service or non-party products that are required to enable Company to access the Network (each, a "Network Suspension").

(k) **No Liability for Network Service Suspension**. Panasonic will not be liable to Company or any Authorized User for any damage, liabilities, losses (including any loss of data or profits), or any other consequences that Company or any Authorized User may incur or sustain because of a Network Suspension.

8. **Intellectual Property rights**. Subject to the limited rights expressly granted under this Policy, PAC reserves all right, title and ownership interest in and to the Network, all content therein, and all Confidential Information, including all related Intellectual Property Rights. No rights are granted to Company other than as expressly stated in this Policy. As used in this Policy, "**Intellectual Property Rights**" means any patent, copyright, trademark, trade secret, utility certificate, utility model, database right, industrial design right, and all registrations, applications, renewals, extensions, combinations, divisions, continuations or any derivative works or reissues of them, whether arising by operation of law, treaty, contract, license or otherwise.

9. **Termination of Access**. PAC may terminate Company's access to the Network or Site immediately if it deems that termination is reasonably necessary in its sole judgment to protect the security or its own use of the Network or the Site.