SWARM NETWORK PRACTICES GUIDE

1. **Purpose**. This Swarm Network Practices Guide ("Guide") sets forth the policies for operation of the Swarm Network including the provisioning of Swarm Hardware and access to the data carried by the Swarm Services. Swarm reserves the right to modify and update this Guide at any time.

   This Guide is incorporated by reference into and forms part of the applicable agreement with Swarm Technologies, Inc. for Swarm Hardware and Swarm Services ("Agreement"). For avoidance of doubt, a Customer may be a Value-Added Reseller, Distributor, Subscriber, or End-User, whichever the case may be ("Customer"). It is the responsibility of such Customer to be aware of the most recent version of this Guide.

2. **Definitions.** All capitalized terms not otherwise defined herein have the meanings assigned to them in the Agreement. In the event of a conflict with this Guide, the Agreement shall take precedence.

3. **Network Operations.**

   3.1. Swarm will provide Customer with product and service information relating to the Swarm Network. Customer will, as applicable, represent product and service information in accordance with the stated functionality and performance.

   3.2. Disruptions in Swarm Services: The provision of service to Customer relies on the proper functioning of Customer's equipment and services as well as the proper functioning of the equipment and services of the Swarm Network not under Customer's control. If Customer has Subscribers, Customer's obligations to provide service to its Subscribers is subject to each of the following:

   3.2.1. Proper functioning of the Swarm Network and any third-party telecommunications carrier, facility, or other such capability required to operate the Swarm Network.

   3.2.2. The availability of capacity on the Swarm Network over time and geographic locations.

   3.3. System Limitations: The following constraints apply to the ability to provide Swarm Services:

   3.3.1. Access to the Swarm Network may be refused or limited, without liability on the part of Swarm, due to capacity limitations, including limitations due to, but not limited to, use by other Customers, use by Subscribers (as applicable), repair, testing, upgrade or modification of the Swarm Network.

   3.3.2. Emergency access to the Swarm Network by public safety or governmental organizations when so approved or required under law.

   3.4. Swarm Services Outages: Swarm Services outages affecting the core Swarm Network that prevent messages being delivered to or from the Swarm Hardware will be reported to Customer. Outages that affect individual satellites or gateways will not be reported. It is the responsibility of Customer to ensure that they are correctly receiving outage notifications from

Swarm. Notifications will only be available to Customer via email, through Swarm's online notification platform.

3.4.1. Planned Outages: Swarm will provide advance notice of planned outages, as set forth in the Agreement.

4. Swarm Hardware.

4.1. Customer will only obtain Swarm Hardware from Swarm in accordance with Swarm's published sales terms and conditions, or from a vendor specifically approved in writing by Swarm to sell the Swarm Hardware.

4.2. Before distributing any Swarm Hardware, if applicable to Customer, Customer will ensure that the identification number of the Swarm Hardware is correctly documented and recorded on any Swarm Network database required by Swarm.

4.3. Customer shall not create, attempt to create, or cause another entity to create its own version of Swarm Hardware without written approval of Swarm.

5. Provisioning.

5.1. Swarm shall provide Customer with access to Swarm's online device registration tool; the Swarm Hive. Customer shall ensure it maintains security of the access credentials and limits access to the provisioning tool to specific authorized personnel only.

5.2. If and as applicable, Customer shall only register and commercially activate Products using the Swarm Hive and its associated Application Programmable Interface (API).

5.3. Customer will maintain a database of service requests, such as Swarm Hardware device ID numbers, dates, types of service requests, and feature selections. Customer can submit service requests by emailing support@swarm.space.

5.4. Swarm maintains a list of device IDs for all Swarm Hardware. The device ID is stored in a database, and references the hardware and firmware equipment status and is also used to minimize fraud from lost or stolen Swarm Hardware. Customer is responsible for notifying Swarm, along with adequate documentation, of lost or stolen Swarm Hardware and the related Swarm Hardware device ID. Only Swarm Hardware on Swarm's device ID list can be activated on the Swarm Network. Customer shall notify Swarm within twenty-four (24) hours of learning of lost or stolen Swarm Hardware.

6. Access to Data: Customer is responsible for collecting data and sending data to the Swarm Network for the Swarm Hardware provisioned by Customer via the Application Programmable Interface (API) made available by Swarm.

7. Customer Support.

7.1. Customer, if and as applicable:

7.1.1. Customer is responsible for resolving all Subscriber problems related to Subscriber's use of the Product. If Customer determines that a problem cannot be resolved by it and is related to the Swarm Hardware, Swarm Services, or the Swarm Network, Customer will promptly contact Swarm and open a support ticket.

7.2. Unless otherwise provided in the Agreement, Swarm will only provide support to Customers with a direct contract with Swarm. Any other party that contacts Swarm will be referred to the entity from which that party obtained the Swarm Services and or the Swarm Hardware.

7.2.1. Method of Contact: Customer shall have the option to contact Swarm support via email at support@swarm.space.

8. Default of Agreement: In the event of a material breach of the Agreement by Customer, Swarm will remove Customer's access to provisioning capabilities and may also remove Customer's ability to connect to the Swarm Network.

9. Security and bypass.

9.1. Customer will, as applicable to the specific Customer:

9.1.1. Establish commercially reasonable security measures to minimize the likelihood of any fraudulent or unauthorized access, including bypass, to any element of the Swarm Network. Such security measures shall include perimeter security, Swarm Network scanning, malware, virus detection, and intrusion detection capabilities.

9.1.2. Establish reasonable, comprehensive security measures to any information technology capability used by Customer in providing Swarm Services to Subscribers.

9.1.3. Establish an effective inventory security control program to protect Swarm Hardware stored at any location, or in transit between locations. An effective program accounts for chain of custody of inventory through periodic reconciliation of inventory records.

9.1.4. Promptly notify Swarm of any actual or suspected fraudulent activity, security issue, unauthorized activity or issue that may affect normal operations of any aspect of the Swarm Network, any infrastructure used by the Swarm Network, or any services used by the Swarm Network.

9.1.5. Comply with commercially reasonable security requirements set by Swarm relative to access and use of the Swarm Network by Customer (and Customer's Subscribers, if applicable).

9.1.6. Cooperate with Swarm's investigation of issues that in Swarm's sole judgement, constitute fraudulent or unauthorized access, bypass, network abuse, damage or potential damage to any part of the Swarm Network, abnormal wear and tear, abnormal service

performance, network congestion, or other similar fraud and abuse issues as may be described in the Agreement. Customer shall also require its distributors, agents, and Subscribers to cooperate in said investigation.

9.2 Swarm will establish commercially reasonable security measures to minimize likelihood of any fraudulent or unauthorized access, including bypass, to any element of the Swarm Network.

10. Fair Access Policy, Prohibited Uses and Activities, Network and Usage Restrictions.

10.1. Swarm reserves the right to actively monitor usage statistics of the Swarm Hardware on the Swarm Network and take proactive measures to regulate, and if necessary, suspend or deactivate Swarm Hardware to ensure high quality Swarm Network performance. The purpose of Swarm's Fair Access Policy ("Policy") is to set forth its expectations for reasonable use of the Swarm Network that is in the best interest of all Customers, as solely determined by Swarm, and to reduce or eliminate excessive use or misuse of the Swarm Network that may negatively affect other Customers or the performance of the Swarm Network.

10.2. Prohibited Uses and Activities. Customer's use of the Swarm Network, Swarm Services, and Swarm Hardware under the Agreement may not diminish or interfere with the fair use of the Swarm Network by any other parties, be illegal, or infringe on the rights of others. Customer's Subscribers must comply with this Policy. Failure to comply with this Policy may result in the suspension or termination of the Swarm Services associated with the relevant Swarm Hardware used or operated by Customer (and/or Customer's Subscribers) as solely determined by Swarm. Prohibited uses and activities of the Swarm Services include, but are not limited to:

10.2.1. Using the Swarm Network for any unlawful purpose. This includes the transmittal or dissemination of data, material or information which constitutes or encourages a criminal offence or violates any applicable local, state, federal, U.S., international law, regulation, or order.

10.2.2. Causing unreasonably large amounts of data to be transmitted on the Swarm Network, as solely determined by Swarm.

10.2.3. Any activity that causes abnormal wear and tear to the Swarm Network, denial of service attack(s), distribution of malware, viruses, spyware, worms, Trojans, adware, back doors, that cause a reduction in capacity of the Swarm Network.

10.2.4. Attempting to communicate with Swarm Hardware that was not provisioned by Customer.

10.2.5. Servicing, altering, modifying, or tampering with the Swarm Hardware unless such servicing is approved in writing by Swarm or such modification is clearly documented in the most recent version of the documentation for the Swarm Hardware.

10.2.6. Reverse engineering or assisting or facilitating any other party in the reverse engineering of any part of the Swarm Network, Swarm Hardware, or Swarm Services.

10.3. Customer Conduct. Customer is responsible for its compliance with the Policy as well as, if applicable, any use or misuse of Swarm Service by its Subscribers or anyone else Customer has permitted to access the Swarm Network, Swarm Hardware, or Swarm Services.

10.3.1. In every case, Customer is responsible for the security of any Product, Swarm Hardware or any data stored on Swarm Hardware, or Swarm Services, that Customer provisions on the Swarm Network.

10.4. Violation of Guide and Policy. Swarm reserves the right to:

10.4.1. Refuse to transmit and to block any information or data that, in its sole discretion, is a violation of the Policy or otherwise harmful to the Swarm Network irrespective of whether such data or information is lawful or not.

10.4.2. Monitor activity on the Swarm Network, Swarm Services, or Swarm Hardware for, but not limited to, validating access credentials, determining usage data for Swarm Network operation, planning, research, marketing, financial, maintenance, and any other reasonable business purpose.

10.4.3. Monitor and investigate any activity in Customer's account(s) for violations, and to document, disclose, block, or remove such violations in accordance with this Guide, the Policy, the Agreement, and applicable law.

10.4.4. Take commercially reasonable actions, to ensure high quality Swarm Network performance for all Swarm Network users, if it becomes aware of inappropriate use of the Swarm Hardware, Swarm Services, or the Swarm Network. Swarm prefers to inform Customer of inappropriate activities and provide a reasonable period for corrective action to occur. However, if the Swarm Services are used in any way that Swarm, in its sole discretion, believes violates this Guide or the Policy, Swarm may take any actions that it deems appropriate under the circumstances with or without notice. These actions include, but are not limited to, the immediate suspension or termination of all or any portion of the Swarm Services or Swarm Hardware. Swarm will have no liability for any reasonable action taken. These actions are not Swarm's exclusive remedies and Swarm may take any other legal or technical actions it deems appropriate with or without notice, and as may further be set forth in the Agreement.

10.4.5. Immediately suspend or terminate Customer's Swarm Services account and the Agreement if Customer, or anyone else Customer permits to access the Swarm Services, violates this Guide, the Policy, the Agreement, or applicable law without recourse. In such event, Customer will receive no compensation for unused, prepaid Swarm Services. Any initial sales or purchase incentives for the applicable Swarm Hardware will be forfeited and charged back to Customer.

10.5. The use of the Swarm Services for emergency or critical communications activities is prohibited.