ACCEPTABLE USE POLICY

This Acceptable Use Policy ("AUP" or "Policy") describes actions by Users that are prohibited by Secure Cloud Video and its affiliates and subsidiaries. "Users" means any User or Customer of any and all Secure Cloud Video provided services ("Service" and/or "Services") that are provided by Secure Cloud Video pursuant to any applicable customer agreement, including, without limitation, any applicable terms of service and/or supplements to any applicable agreement(s) (which Users must accept as a condition to receiving any Services from Secure Cloud Video).

This Acceptable Use Policy is subject to change from time to time with such changes effective upon posting at http://securecloudvideo.com/index.php/policy. Secure Cloud Video encourages Users to review this Policy regularly.

1.0 Services may be used only for lawful, proper and appropriate purposes.

- Users must use any Service only in a manner that, in Secure Cloud Video sole discretion, is consistent with the purposes of such Services. Users will not engage in any legal or illegal activity that either (i) harms Secure Cloud Video, the network operated by Secure Cloud Video, the Services and/or any User, or (ii) interferes with the network operated by Secure Cloud Video and/or the provision or use of the Services by Secure Cloud Video or any User.

1.1 Services may not be used for illegal, improper, and/or inappropriate purposes.

Illegal purposes include, but are not limited to:

- Using the service to violate any law, rule, or regulation; or engaging in threatening, abusive, harassing, defamatory, libelous, deceptive or fraudulent behavior.

1.2 Customer shall not:

(1) Re-classify or re-originate video or audio or take any other action to make video or audio appear as if it:

(i) originated from a place or on a type of equipment different from the place or type of equipment from where it, in fact, originated; or

(ii) modify, alter, or delete in any manner the video or audio recording. Upon Secure Cloud Video's request, Customer shall certify in writing its continued compliance with this Policy. If Customer is found to be in violation of the above policy then Customer must demonstrate to Secure Cloud Video's satisfaction that all video or audio recordings are compliant to this policy or Customer may be subject to penalties assessed retroactively to include all instances of policy violation.

1.3 Engaging in any of the foregoing activities by using the services of another provider or third party and channeling such activities through an account provided by Secure Cloud Video, or otherwise involving the Services or any Secure Cloud Video account in any way with or without another provider or third party for the purpose of facilitating the foregoing activities.

2.0 Remedies

- Secure Cloud Video reserves the right, at its sole discretion, to determine if a Service is being used for any of the foregoing purposes or activities.

- Violation of this Policy may result in civil or criminal liability, and Secure Cloud Video in its sole discretion, in addition to any remedy that it may have at law or in equity, may immediately terminate permission for the User to use the Services, or any portion of the Services, and may charge User any applicable rates and cancellation or termination fees. In addition, Secure Cloud Video may investigate incidents that are contrary to this Policy and provide requested information to third parties who have provided notice to Secure Cloud Video stating that they have been harmed by a User's failure to abide by this Policy or the policies listed above. Secure Cloud Video may bring legal action to enjoin violations and/or collect damages caused by any violation of any part of this Policy.
- Any violations or attempted violations of this Policy by any User (or any third party on behalf of any User) will constitute a violation of this Policy by the User and a material breach of any applicable customer agreement, including, without limitation, any applicable terms of service and/or supplements to any applicable agreement(s).
- Secure Cloud Video's failure to enforce this policy in every instance in which it might have application does not amount to a waiver of Secure Cloud Video rights
- IN NO EVENT WILL SECURE CLOUD VIDEO BE LIABLE TO ANY USER OR THIRD PARTY FOR ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES FOR ACTIONS TAKEN OR NOT TAKEN PURSUANT TO THIS POLICY, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR DATA, OR OTHERWISE, EVEN IF SECURE CLOUD VIDEO WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY IN FAVOR OF Secure Cloud Video IS IN ADDITION TO ANY LIMITATIONS SET FORTH IN ANY WRITTEN AGREEMENT BETWEEN Secure Cloud Video AND ANY APPLICABLE USER AND WILL APPLY WHETHER THE ACTION IN WHICH RECOVERY IS SOUGHT IS BASED IN CONTRACT OR TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE OR STRICT LIABILITY), OR ANY APPLICABLE LAWS.

3.0 Export Restrictions

- You acknowledge and agree that the software and/or hardware used in conjunction with the Plan Services may be subject to Canada, United States and other foreign Laws and regulations governing the export, re-export, and/or transfer of software by physical or electronic means. You agree, represent, covenant, and warrant that:

  (i) neither You nor any End User (nor any entity or person that controls You or any End User):

  (a) is located in an Embargoed Area or listed on any Export Control List or

  (b) will export or re-export any Secure Cloud Video software or hardware into any Embargoed Area or to any person, entity, or organization on any Export Control List, or to any person, entity, or organization subject to economic sanctions due to ownership or control by any such person, entity, or organization, without prior authorization by license, or license exemption and;

  (ii) The Plan Services and Secure Cloud Video software and/or hardware will not be used or accessed from any Embargoed Area.

4.0 Video and Audio Recordings

- Features of Video and Audio Services with Secure Cloud Video allows you or users of the Services to record Video and Audio or other communications. The notification and consent requirements relating to the recording of Videos and/or other communications may vary from state to state and country to country.

You should consult with an attorney prior to recording any Video or Audio as some states or countries may require users to obtain the prior consent of all parties to a recording, or other Video or Audio communication before the public or Employee are recorded. You represent, covenant and warrant that You will review all applicable Laws before You use or allow use of the Plan Services to record any videos or other audio communications and will at all times comply with all applicable laws. You agree to inform all users of Your Account that they are obligated to comply with all Laws relating to their use of the call recording feature.

- Violations of the call recording Laws may be subject to criminal or civil penalties.
- To store PHI (Personal Health Information); or if You qualify as a "covered entity," "business associate," or "subcontractor" under HIPAA (or similar terms under similar legislation in other jurisdictions), or are otherwise subject to HIPAA, to transmit, receive, or store PHI without the Secure Cloud Video HIPAA Conduit setting being active and in effect.
- A breach of obligations in this Section constitutes a material breach of these AUPs, as applicable, such that Secure Cloud Video may suspend service, terminate the Agreement immediately, or take any other action Secure Cloud Video deems necessary to enforce the terms of this Section.

5.0 Prohibited Acts

- You represent, warrant, covenant, and agree that neither you nor any End User shall do any of the following during the Term:
    - Transmit, upload, distribute in any way, or store any corrupted file or material that contains viruses, time bombs, Trojan horses, worms, malware, spyware, or any other programs or materials that may be harmful or dangerous or may damage the operation of the Plan Services or another party's computers, devices, equipment, systems, or networks;
    - Take advantage of, bypass, exploit, or otherwise avoid Your obligations or the provisions, restrictions, and prohibitions set forth in this Section 6 (or attempt to do so);
    - Interfere with or disrupt networks or systems connected to the Plan Services;
    - Sell; resell; distribute; lease; export; import; or otherwise grant or purport to grant rights to third parties with respect to the Plan Services, and any software or hardware used in conjunction with the Plan Services or any part thereof without Secure Cloud Video's prior written consent;
    - Display or use of any Secure Cloud Video Mark in any manner in violation of Secure Cloud Video's then-current policies on its trademark and logo usage or without Secure Cloud Video's express, prior written permission, to be granted or denied in Secure Cloud Video's sole discretion,
    - Display or use of any Third Party Mark without the prior, written consent of the third party that owns the Third Party Mark;
    - Undertake, direct, attempt, cause, permit, or authorize the modification, creation of derivative works, translation, reverse engineering, decompiling, disassembling, or hacking of the Plan Services or any software and hardware used in conjunction with the Plan Services, or part thereof;
    - Defeat, disable, or circumvent any protection mechanism related to the Plan Services;
    - Intercept, capture, sniff, monitor, modify, emulate, decrypt, or redirect any communication or data used by Secure Cloud Video for any purpose, including without limitation by causing any product to connect to any computer server or other device not authorized by Secure Cloud

Video or in any manner not authorized in advance in writing by Secure Cloud Video;

- Allow any service provider or other third party – with the sole exception of Secure Cloud Video authorized maintenance providers acting with Secure Cloud Video express, prior authorization – to use or execute any software commands that facilitate the maintenance or repair of any software or hardware used in conjunction with the Plan Services;
- Gain access to or use (or attempt to gain access or use) any device, system, network, account, or plan in any unauthorized manner (including without limitation through password mining);

- A breach of obligations in this Section constitutes a material breach of these AUPs, as applicable, such that Secure Cloud Video may suspend service, terminate the Agreement immediately, or take any other action Secure Cloud Video deems necessary to enforce the terms of this Section.