Acceptable Use Policy (AUP)

This Acceptable Use Policy ("**AUP**") is part of the Platform as a Services Agreement between Customer and Essential (the "**Agreement**"). This AUP applies to use of the Essential Services by Customer and its Users.

Customer's and/or its Users access to and use of Essential Services may be suspended or terminated for violation of this AUP, as further specified in the Agreement.

Capitalized terms used in this AUP have the meaning given in the Agreement.

A. Use of the Services

Neither Customer nor its Users may:

- Interfere or attempt to interfere in any manner with the functionality or proper working of the Services;
- Upload to the Essential Services, or use the Essential Services to store, process or transmit material in violation of third-party privacy or data protection rights;
- Upload to the Essential Services, or use the Essential Services to store, process or transmit any malware. Malware means programming (code, scripts, active content, and other software) that is designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, or gain unauthorized access to system resources, or that otherwise exhibits abusive behavior. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, or other malicious or unwanted software or programs;
- Upload to the Essential Services, or use the Essential Services to store, process or transmit any Protected Health Information in a way that violates the Health Insurance Portability and Accountability Act of 1996;
- Use the Essential Services in any manner that violates industry standards, including the guidelines published by the Cellular Telephone Industries Association ("CTIA"), the Mobile Marketing Association, carrier guidelines, or any similar or analogous industry standards, third party policies or requirements;
- Use the Essential Services to engage in any unsolicited advertising, marketing or other activities, including to send unsolicited mass mailings outside its organization, and including any activity that violates the CAN SPAM Act of 2003, the Telephone Consumer Protection Act, the Do-Not-Call Implementation Act, or any similar or analogous anti-spam, do-not-call, telemarketing, auto-dialing, data protection, or privacy legislation. The term "unsolicited mass mailings" includes all statutory or common definitions or understanding of those terms in the applicable jurisdiction, including without limitation, those set forth for "Commercial Electronic Mail Messages" under the U.S. CAN-SPAM Act;
- Use the Essential Services to create a false identity, forged email address or header, false phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or telephone call;
- Interfere with or disrupt the integrity or performance of the Essential Services or third-party data stored or processed with the Services or attempt to gain unauthorized access to the Essential Services or their related systems or networks; or
- Attempt to probe, scan, penetrate or test the vulnerability of any Essential system or network (including those of its service providers), or to circumvent, avoid or breach Essential's or its service providers' security or authentication measures, whether by passive or intrusive techniques, or by social engineering, without Essential's express prior written consent.

B. Shared Resources

Neither Customer nor its Users may use Essential systems, networks or technology in a way that unnecessarily interferes with their normal operation, or that consumes a disproportionate share of their resources. Customer agrees that Essential may quarantine or delete any data stored on Essential's systems or networks if Essential reasonably believes that the data is infected with any malware, or is otherwise corrupted, and has the potential to infect or corrupt Essential systems, networks or technology or other customers' data that is stored or accessed via Essential systems, networks or technology. Customer and its Users will comply with any written security or network access requirements that Essential provides to Customer in connection with its use of the Essential Services.

C. Other Networks

Customer and its Users must comply with the rules of any other network its accesses or participates in when using the Essential Services.

D. Abuse

Neither Customer nor its Users may use Essential's network or services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including:

- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network;
- Monitoring data or traffic on any network or system without the express authorization of the owner of the system or network;
- Interference with service to any user of the Essential or other network including mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
- Use of an Internet account or computer without the owner's authorization;
- Collecting or using email addresses, phone numbers, screen names or other identifiers without the consent of the person identified (including, phishing, Internet scamming, password robbery, spidering, and harvesting);
- Collecting or using information without the consent of the owner of the information;
- Use of any false, misleading, or deceptive TCP-IP packet header information in an email or a newsgroup posting;
- Use of the Services to distribute software that covertly gathers information about a user or covertly transmits information about the user; or
- Any conduct that is likely to result in retaliation against the Essential network or website, or Essential's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS).

E. Offensive Content

Neither Customer nor its Users may publish, transmit or store on or via Essential's network or equipment any content or links to any content that Essential reasonably believes:

- Is obscene;
- Contains harassing content or hate speech, or is violent, incites violence, or threatens violence;
- Is unfair or deceptive under the consumer protection laws of any jurisdiction;
- Is defamatory or violates a person's privacy;
- Creates a risk to a person's safety or health, creates a risk to public safety or health, is contrary to applicable law, or interferes with a investigation by law enforcement;
- Improperly exposes trade secrets or other confidential or proprietary information of another person;
- Is intended to assist others in defeating technical copyright protections;
- Infringes on another person's copyright, trade or service mark, patent, or other property right, or violates any privacy right;
- Is illegal or solicits conduct that is illegal under laws applicable to you or to Essential; or
- Is otherwise malicious, fraudulent, or may result in retaliation against Essential by offended viewers or recipients.

F. Other

If Customer or any User knows of any violation of this AUP, then they must immediately notify Essential by contacting info@essential.to. Customer will not be entitled to any credit or other compensation for any interruptions of service resulting from AUP violations.