ACCEPTABLE USE POLICY (AUP) FOR THE WALR PLATFORM

1. AUP INTRODUCTION

1.1. The main objectives of this AUP are to provide Walr Clients with reliable and stable access to the Walr Platform accessed On-Demand (the "Service") and to protect the privacy and security of Clients' data and information.

1.2. While it is not Walr's intent to actively monitor Clients' use of the Service, Walr may take such actions as deemed appropriate by it when it becomes aware of a violation of this AUP.

1.3. This AUP supplements, but does not supersede, the Documentation, as well as the Walr Terms & Conditions (the "Agreement") that Client has executed with Walr. If the Documentation or the Agreement restricts the use of the Service in areas not addressed in this AUP, the Documentation or the Agreement will govern with respect to such areas.

2. PROHIBITED USE

2.1. Illegal and Criminal Activity / Security Violations / Threats

Client may not use the Service to engage in illegal, abusive, or irresponsible behaviour, including but not limited to:

- 2.1.1. criminal or civil violations of state, federal, or international laws, regulations, or other government requirements where such violations include but are not limited to theft or infringement of copyrights, trademarks, trade secrets, or other types of intellectual property; fraud; forgery; theft or misappropriation of funds, credit cards, or personal information;
- 2.1.2. unauthorised access to or use of data, services, systems or networks, including any attempt to probe, scan or test the vulnerability of either the Service or another system or network or to breach security or authentication measures, without express prior written authorisation of the owner of the system or network;
- 2.1.3. interference to the Service or any user, host or network including, without limitation, mail bombing, flooding, and deliberate attempts to overload a system;
- 2.1.4. use of an Internet account or computer without the owner's authorisation;
- 2.1.5. collecting information by deceit, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, phishing, security hole scanning, and port scanning;
- 2.1.6. use of any false, misleading or deceptive TCP-IP packet header or any part of the header information in an email or a newsgroup posting;
- 2.1.7. use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- 2.1.8. any activity or conduct that is likely to result in retaliation against the Service or Walr;
- 2.1.9. introducing intentionally or knowingly into the Service any virus, contaminating program or script code; or fail to use an up to date virus-scanning program on all material downloaded from the Services;
- 2.1.10. transmission of materials of threatening nature, including threats of death or physical harm, harassment, libel, racism, sexual or religious discrimination, and defamation; or
- 2.1.11. any other activity or conduct that unreasonably interferes with the Service, or other customers' use of our Service.

2.2. Offensive Content

Client may not publish, display or transmit via the Service any content that Walr reasonably believes:

- 2.2.1. is unfair or deceptive under the consumer protection laws of the applicable jurisdiction, including chain letters and pyramid schemes;
- 2.2.2. is defamatory or violates a person's privacy;
- 2.2.3. creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement bodies;
- 2.2.4. improperly exposes trade secrets or other confidential or proprietary information of another person;
- 2.2.5. is intended to assist others in defeating technical copyright protections;
- 2.2.6. infringes another person's trade or service mark, patent, or other property right;
- 2.2.7. is discriminatory in any way, including by way of sex, race, or age discrimination;
- 2.2.8. constitutes or encourage child pornography or is otherwise obscene, sexually explicit or morally repugnant;
- 2.2.9. facilitates any activity or conduct that is or may be defamatory, pornographic, obscene, indecent, abusive, offensive or menacing;
- 2.2.10. is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;
- 2.2.11. involves theft, fraud, drug-trafficking, money laundering or terrorism;
- 2.2.12. is otherwise illegal or solicits conduct that is illegal under laws applicable to Client or to Walr; and
- 2.2.13. is otherwise malicious, fraudulent, or may result in retaliation against CONIFIRMIT by offended viewers.

"Publish, display or transmit via the Service" includes web content, email, and any other type of posting, display or transmission, direct or by means of references, that relies on the Internet.

2.3. Copyrighted Material

Client may not use the Service to publish, distribute, or otherwise copy in any manner any text, music, software, art, image or other work protected by copyright law unless Client:

- 2.3.1. has been expressly authorised by the owner of the copyright for the work to copy the work in that manner; and
- 2.3.2. is otherwise permitted by copyright law to copy the work in that manner.

2.4. Emailing and Spam

- 2.4.1. The Service may only be used to perform the following types of email send-outs:
  - 2.4.1.1. invitations to surveys actually hosted on the Service (except where otherwise agreed to by Walr in writing), and reminders thereof;
  - 2.4.1.2. thank-you emails sent upon completion of a survey hosted on the Service;
  - 2.4.1.3. dispatching of exports (data-files or graphical reports) from surveys hosted on the Service
- 2.4.2. The laws and rules applicable to each individual Client, will depend on the laws in the jurisdictions to which emails are being sent by Client, and include e.g. CAN-SPAM Act of 2003 in the US, or the European Directive 2002/58/CE of 12 July 2002 on privacy and electronic communications. Following are some (but not all) activities that are strictly prohibited:
  - 2.4.2.1. sending unsolicited or undesired email messages ("spam")

2.4.2.2. sending email without providing in the email itself a simple way of requesting to be excluded from receiving additional emails from the originator of the email ("opt out");
2.4.2.3. sending emails that do not accurately identify the sender's name, the sender's return address, and the email address of origin, or in general misrepresenting oneself;
2.4.2.4. sending email for the primary purpose of commercial advertising or promotion, independent of whether a Walr survey is referred to or used;
2.4.2.5. sending email with charity requests, petitions for signatures, or any chain mail related materials; and
2.4.2.6. collecting the responses from unsolicited email.

3. CONSEQUENCES OF (i) PROHIBITED USE, AND (ii) REGULATIONS OF USAGE

3.1. Violations by Client, including use by your customers, of the regulations in Articles 2 of this Schedule may result in (i) immediate removal of offending materials; (ii) blocked access to, or partial or full suspension of Service; or (iii) other actions appropriate to the violation, as determined by Walr in its sole discretion. Walr shall make reasonable efforts to contact Client so that violations may be addressed voluntarily by Client however Walr reserves the right to act without notice when necessary to preserve the stable, secure and uninterrupted operations of the Service, as determined by Walr at its sole discretion.

3.2. Client may be requested by Walr to bring the offending or breaching materials in compliance with this AUP and the Agreement. Any costs incurred by Client in conjunction with this shall be borne solely by Client.

3.3. Walr may involve, and will cooperate with, law enforcement agencies and government agencies if criminal activity is suspected. Violators may also be subject to civil or criminal liability under applicable law.

3.4. With the exception of Walr's gross negligence of willful misconduct, Walr shall have no liability whatsoever to Client in connection with actions taken by Walr in the wake of Client's violation of this AUP. Furthermore, Client shall not be entitled to any compensation under the Service Level Agreement if the cause of the issue is a breach of the AUP by Client.

3.5. Walr will charge Client at its standard rates for Additional Services for work necessitated by it and related to breaches of the AUP by Client. Charges will be applied reasonably, but repeated offences will be charged in full. Charges may e.g. apply when Walr is to (i) investigate or otherwise respond to any apparent or actual violation of this AUP by Client; (ii) remedy harm caused to Walr or any of its other customers by the use of Client of the Service in violation of this AUP or the Agreement; (iii) respond to third party complaints related Client's use of the Service in breach of the AUP; and (iv) work related to removal of Walr's Internet Protocol numbers from any "blacklist" in the wake of Client's actions.

4. INCIDENT REPORTING

4.1. Any complaints regarding violations of this AUP by a Client should be directed to legal@walr.com, and where possible, include details that would assist in investigating and resolving the complaint.

5. REVISIONS OF THIS AUP

5.1. Walr may modify this AUP at any time with thirty (30) days prior email notification to Designated Users. Such modifications will be effective when posted to Walr's web site.