

RETHINKEHS
ACCEPTABLE USE POLICY

This Acceptable Use Policy (AUP) describes activities that are required or allowed on Rethink Safety, Inc. (RETHINK) network; it also provides cautions against activities that RETHINK network shall not allow. This AUP is part of the Agreement between CLIENT and RETHINK, and the latter may suspend or terminate the Agreement for any violation of this AUP.

1. GENERAL STATEMENT

The provisions of this AUP are intended as guidelines. CLIENT shall also comply with applicable laws and regulations, as well as with general standards of behaviour in using the Internet.

2. CAUTIONS AGAINST ABUSE

CLIENT shall not use RethinkEHS and Services to engage in, foster, or promote illegal, abusive, or irresponsible behaviour, including but not limited to unauthorized access to or use of data, services, systems or networks, including any attempt to probe, scan or test the system or network or to do or perform acts that may breach RethinkEHS security and authentication measures; unless with written authorization of RETHINK; such acts and behaviour may consist of, but are not limited to:

- a. interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
- b. collecting information by deceit, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, phishing, security holescanning, and port scanning;
- c. use of the Services to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- d. any activity or conduct that is likely to result in retaliation against RETHINK's network;
- e. any activity or conduct that is likely to be in breach of any applicable laws, codes or regulations including data protection;
- f. introducing intentionally or knowingly into the system any virus or other contaminating code.

3. SECURITY

CLIENT shall take reasonable security precautions, including but not limited to the following:

- a. Comply with best business practices for password security; and
- b. Scan all materials stored or transmitted using RethinkEHS and Services for viruses, worms, Trojan horses and other malicious codes using a commercially recognized and up-to-date scanning program or service. CLIENT must remove or quarantine any content that is corrupted with malicious code immediately upon discovery.

- c. Immediately notify RETHINK of any breach in security of the system or network, and not attempt to do anything with the system without knowledge of RETHINK, without RETHINK representative present or without RETHINK representative performing the correction him/herself.

4. VULNERABILITY TESTING

CLIENT shall not attempt to probe, scan, penetrate or test the vulnerability of RETHINK's system or network or to breach its security or authentication measures, whether by passive or intrusive techniques without RETHINK's prior written consent.

5. CAUTIONS AGAINST ABUSIVE CONTENT

Content "published or transmitted" via RETHINK's network includes Web content, bulletin board postings, chat, and any other type of posting, display or transmission that relies on the Internet. CLIENT shall not publish, display or transmit via RETHINK's network any content or links to content that the latter reasonably believe may:

- a. be unfair or deceptive under the consumer protection laws of any jurisdiction, or include chain letters and pyramid schemes;
- b. be defamatory or violate a person's privacy or any right of publicity;
- c. create a risk to a person's safety or health, create a risk to public safety or health, compromise national security, be likely to cause or encourage public disorder, or interfere with an investigation by law enforcement bodies;
- d. improperly expose trade secrets or other confidential or proprietary information of another entity or person;
- e. constitute unfair competition.

6. DATA PRIVACY

- a. CLIENT shall ensure that all the personal information, or any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual, collected, accessed, processed and used by CLIENT and hosted through the Software and Services shall comply with the Data Privacy Act of 2012.
- b. CLIENT shall not engage in any activities or actions that would violate the personal privacy rights of others, including but not limited to, collecting and distributing information about Internet users without their permission, except as permitted by applicable law.
- c. CLIENT acknowledges and agrees to inform its customers about RETHINK's possible use of the data collected by necessity for RETHINK's provision of the RethinkEHS.

7. INTELLECTUAL PROPERTY AND OTHER PROPRIETARY RIGHTS

CLIENT shall not use RethinkEHS in a manner that infringes on or misappropriates the rights of a third party in any work protected by copyright, trade or service mark, invention, or other intellectual property or proprietary information. For example:

- a. CLIENT shall not use RethinkEHS to download, publish, distribute, use, or otherwise copy in any manner any text, music, software, art, image, or other work protected by copyright law unless CLIENT has permission from the owner of the work to use or copy the work in that manner, or CLIENT is otherwise permitted by established intellectual property law to copy or use the work or rights in that manner;
- b. CLIENT shall not use RethinkEHS to publish content intended to assist others in defeating technical copyright protections; and
- c. CLIENT shall not display another entity's or person's trademark without permission.

In addition, CLIENT shall not use RethinkEHS to publish another entity's or person's trade secrets, or to publish information in violation of a duty of confidentiality.

8. COOPERATION WITH INVESTIGATIONS AND LEGAL PROCEEDINGS

RETHINK shall monitor any content or traffic transmitted via RethinkEHS as part of its investigation of a suspected AUP violation. Should RETHINK be legally required to permit any relevant authority to inspect CLIENT's content or traffic, CLIENT shall agree that RETHINK can do so; provided however that, where possible, without breaching any legal or regulatory requirement, RETHINK shall give CLIENT reasonable prior notice of such requirement.

9. THIRD PARTY CONDUCT

CLIENT shall be responsible for violations of this AUP by anyone using the RethinkEHS on an unauthorized basis as a result of CLIENT's failure to use reasonable security precautions. CLIENT's use of the RethinkEHS to assist another person in an activity that would violate this AUP if performed by CLIENT is a violation of the AUP.

10. AMENDMENTS TO THE AUP

The Parties acknowledge that the Internet is continually evolving, and the ways in which the Internet may be abused are also still evolving. Therefore, CLIENT agrees that RETHINK may from time to time amend, change to add or modify restrictions to this AUP and/or CLIENT's use of RethinkEHS, provided that the changes are reasonable and consistent with industry norms.

Any revisions to the AUP shall take effect fifteen (15) Business Days from the date of posting, provided that RETHINK shall inform CLIENT at least fifteen (15) Business Days in advance via email. In the event that the change materially and adversely affects CLIENT's ability to use the RethinkEHS, then CLIENT may terminate the Agreement by thirty (30) Business Days' advance written notice.

11. CONSEQUENCES OF VIOLATION OF AUP

Should CLIENT breach the AUP, RETHINK shall have the right to suspend the RethinkEHS without prior notice. Without limiting the foregoing, RETHINK shall also have the right to block any traffic that it reasonably believes is in violation of this AUP.

In addition to any other remedy, RETHINK shall have the right to charge CLIENT with the cost of equipment and material needed to:

- a. investigate or otherwise respond to any suspected violation of this AUP;
- b. remedy any harm caused to RETHINK or any of its clients by the use of the RethinkEHS in violation of this AUP;
- c. respond to complaints; and
- d. have RETHINK's Internet Protocol numbers removed from any "blacklist".

CLIENT agrees that it shall immediately notify RETHINK and take all necessary actions at CLIENT's disposal to prevent activities in breach of the AUP from continuing or happening again once CLIENT becomes aware of the activities.

CLIENT acknowledges that any violation of its obligations under this AUP will cause grave and irreparable injury to RETHINK and that RETHINK shall have the right to resort to the appropriate injunctive or other equitable immediate relief in addition to monetary compensation against CLIENT.

12. DISCLAIMER

RETHINK shall be under no duty, and by this AUP, shall not be deemed to undertake a duty, to monitor or police CLIENT's activities or any of its customer's activities, and RETHINK disclaims any responsibility for any misuse of its network