Crises Control Acceptable Use Policy

Last Updated May 4, 2018

This Acceptable Use Policy ("AUP") describes actions that Crises Control prohibits when any party uses Crises Control's Services. This AUP is incorporated by reference into, and governed by the Terms of Service or other similar written agreement between you (Customer) and Crises Control (the "Agreement"). The Agreement contains definitions of capitalised terms not otherwise defined in this AUP and takes precedence over any conflicting provisions in this AUP.

Policy

You may not use the Crises Control Services without agreeing to this AUP. Thus, you agree not to use, and not to encourage or allow any End User to use, Crises Control Services in the following prohibited ways:

Using the Crises Control Services to encourage any illegal, fraudulent, abusive, or other activities that materially interfere with the business or activities of Crises Control.

Attempting to bypass or break any security mechanism on any of the Crises Control Services or using the Crises Control Services in any other manner that poses a material security or service risk to Crises Control or any of its other customers.

Reverse-engineering the Crises Control Services in order to find limitations, vulnerabilities, or evade filtering capabilities.

Launching or facilitating, whether intentionally or unintentionally, a denial of service attack on any of the Crises Control Services or any other conduct that materially and adversely impacts the availability, reliability, or stability of the Crises Control Services.

Transmitting any material that contains viruses, Trojan horses, spyware, worms or any other malicious, harmful, or deleterious programs.

Using the Crises Control Services in any manner that materially violates the following: (a) industry standards, policies and applicable guidelines published by (i) the CTIA (Cellular Telecommunications Industry Association), (ii) the Mobile Marketing Association, or (iii) any other generally recognised industry associations; (b) carrier guidelines and usage requirements as communicated in writing by Crises Control to you.

Engaging in any unsolicited advertising, marketing or other activities prohibited by applicable law or regulation covering anti-spam, data protection, or privacy legislation in any applicable jurisdiction, including, but not limited to anti-spam laws and regulations such as the CAN SPAM Act of 2003, the Telephone Consumer Protection Act, and the Do-Not-Call Implementation Act.

Using the Crises Control Services in connection with unsolicited or harassing messages (commercial or otherwise), including unsolicited or unwanted phone calls, SMS or text messages, voice mail, or faxes.

Using the Crises Control Services to harvest or otherwise collect information about individuals, including email addresses or phone numbers, without their explicit consent or under false pretences.

Using the Crises Control Services to engage in, or in connection with fraudulent activity.

Using the Crises Control Services to receive, send or otherwise process Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 as amended, unless you have signed an Associate Agreement with Crises Control or your use of the Crises Control Services fits within the “conduit” or some other exception for requiring a Associate Agreement.

Violating or facilitating the violation of any local, state, federal, or foreign law or regulation, including, but not limited to, laws and regulations regarding the transmission of data or software.

Using the Crises Control Services to transmit any material that infringes the intellectual property rights or other rights of third parties.

Using the Crises Control Services to transmit any material that is, facilitates, or encourages libelous, defamatory, discriminatory, or otherwise malicious or harmful speech or acts to any person or entity, including but not limited to hate speech, and any other material that Crises Control reasonably believes degrades, intimidates, incites violence against, or encourages prejudicial action against anyone based on age, gender, race, ethnicity, national origin, religion, sexual orientation, disability, geographic location or other protected category.

Using the Crises Control Services to transmit any material or content that is offensive, inappropriate, pornographic, obscene or otherwise objectionable to any person or entity who did not provide prior express consent to receive such material or content.

Creating a false identity or forged email address or header, or phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call.

This AUP has examples of restricted behaviour, but does not list all restricted behaviours. Ultimately, Crises Control will decide whether your use violates the AUP.

While we’ve done our best to make our AUP complete, readable, and understandable, you may still have additional questions. We get that. So, feel free to contact our support team at support@crises-control.com.

Or, if you prefer, you may write to us at: Crises Control, 19 heather Park Drive, Wembley, London England, HA0 1SS