Acceptable Use Policy

Usage of Wesurance Services is subject to this Acceptable Use Policy ("AUP"). This Acceptable Use Policy ("AUP") describes activities that are prohibited in connection with your use of the Services. Any users who are found to be violating these rules may see their subscriptions suspended without prior notice. The subscription fees will usually not be refunded.

Section 1 - Illegal or Harmful Use

You may not use Wesurance Services for storing, displaying, distributing or otherwise processing illegal or harmful content. This includes:

1. Illegal activities: You may not offer goods or services, or post or upload Materials, that contravene or that facilitate or promote activities that contravene, the laws of the jurisdictions in which you operate or do business.
2. Harassment, bullying, defamation and threats: You may not offer goods or services, or post or upload Materials, that harass, bully, defame or threaten a specific individual.
3. Hateful content: You may not use the Services to promote or condone hate or violence against people based on race, ethnicity, color, national origin, religion, age, gender, sexual orientation, disability, medical condition, veteran status or other forms of discriminatory intolerance. You may not use the Services to promote or support organizations, platforms or people that: (i) promote or condone such hate; or (ii) threaten or condone violence to further a cause.
4. Intellectual property: You may not offer goods or services, or post or upload Materials, that infringe on the copyright or trademarks of others.
5. Child exploitation: You may not offer goods or services, or post or upload Materials that exploit or abuse children.
6. Malicious and deceptive practices: You may not use the Services to transmit malware or host phishing pages. You may not perform activities or upload or distribute Materials that harm or disrupt the operation of the Services or other infrastructure of Wesurance's third party providers. You may not use the Services for deceptive commercial practices or any other illegal or deceptive activities.
7. Personal and confidential information: You may not post or upload any Materials that contain personally identifiable information, sensitive personal information, or confidential information, such as credit card numbers, confidential national ID numbers, or account passwords unless you have consent from the person to whom the information belongs or who is otherwise authorized to provide such consent.
8. Self-harm: You may not offer goods or services, or post or upload Materials, that promote self-harm.
9. Terrorist organizations: You may not offer goods or services, or post or upload Materials, that imply or promote support or funding of, or membership in, a terrorist organization.

Section 2 - Email Abuse

1. You may not use the Services to transmit unsolicited commercial electronic messages.

Section 3 - Security Violations

You may not attempt to compromise Wesurance Services, to access or modify content that does not belong to you, or to otherwise engage in malicious actions:

1. Unauthorized access: Accessing or using any Wesurance Services without permission
2. Security research: Conducting any security research or audit on Wesurance systems without written permission to do so, including via scanners and automated tools.
3. Eavesdropping: Listening to or recording data that does not belong to you without permission.
4. Other attacks: Non-technical attacks such as social engineering, phishing, or physical attacks against anyone or any system.

Section 4 - Network and Service Abuse

You may not abuse the resources and systems of Wesurance. In particular the following activities are prohibited:

1. Network abuse: Causing Denial of Service (DoS) by flooding systems with network traffic that slows down the system makes it unreachable, or significantly impacts the quality of service

2. Unthrottled RPC/API calls: Sending large numbers of RPC or remote API calls to our systems without appropriate throttling, with the risk of impacting the quality of service for other users.

3. Overloading: Voluntarily impacting the performance or availability of systems with abnormal content such as very large data quantities, or very large numbers of elements to process.

4. Crawling: Automatically crawling resources in a way that impacts the availability and performance of the systems.

5. Attacking: Using the Wesurance services to attack, crawl or otherwise impact the availability or security of third-party systems.

6. Abusive registrations: Using automated tools to repeatedly register or subscribe to Wesurance services, or registering or subscribing with fake credentials, or under the name of someone else.

We may modify this AUP, including the list of Restricted Items, at any time by posting a revised version at https://www.wesurance.io. By continuing to use the Services or access your Account after a revised version of the AUP has been posted, you agree to comply with the latest version of the AUP. In the event of a conflict between the AUP and the Terms, this AUP will take precedence,

but only to the extent required to resolve such conflict. Capitalized terms used but not defined in this AUP shall have the meanings set forth in the Terms.

Section 5 - Reporting Abuse

1. Reports for any abusive behaviour using Wesurance services may be sent to the responsible team via email at contact@wesurance.io