ZENNNN CLOUD — ACCEPTABLE USE POLICY

Last updated: March 20, 2020

Usage of ZENNNN Cloud Services is subject to this Acceptable Use Policy (AUP). This AUP is incorporated by reference into, and governed by the ZENNNN Subscription Agreement between you (Customer) and Nowaday Union Limited, Hong Kong. Customers who are found to be violating these rules may see their subscriptions suspended without prior notice. The subscription fees will usually not be refunded.

Illegal or Harmful Use

You may not use ZENNNN Cloud services for storing, displaying, distributing or otherwise processing illegal or harmful content. This includes:

Illegal Activities
Promoting gambling-related sites or services, or child pornography.

Harmful or Fraudulent Activities
Activities harmful to others, promoting fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, Ponzi and pyramid schemes, phishing, or pharming), or engaging in other deceptive practices.

Infringing Content
Content that infringes the intellectual property of others.

Offensive Content
Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.

Harmful Content
Malicious and malware content, such as viruses, trojan horses, worms, etc.

Spam Content
Content that is published for "black hat SEO" purposes, using tricks such a link building / link spam, keyword spam, in order to exploit the reputation of ZENNNN services for promoting third-party content, goods or services.

Email Abuse

You may not use ZENNNN Cloud services for spamming. This includes:

Unsolicited messages
Sending or facilitating the distribution of unsolicited bulk emails and messages, either directly via ZENNNN Cloud or indirectly via third-party email services. This includes the use of bulk emails lists. Any mass-mailing

activity is subject to the applicable legal restrictions, and you must be able to show evidence of consent/opt-in for your bulk email distribution lists.

Spoofing
Sending emails or messages with forged or obfuscated headers, or assuming an identity without the sender's permission.

Security Violations

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

Unauthorized access
Accessing or using any ZENNNN Cloud system or service without permission.

Security research
Conducting any security research or audit on ZENNNN Cloud systems without written permission to do so, including via scanners and automated tools. Please see our Responsible Disclosure page for more information regarding ZENNNN security research.

Eavesdropping
Listening to or recording data that does not belong to you without permission.

Other attacks
Non-technical attacks such as social engineering, phishing, or physical attacks against anyone
or any system.

Network and Services Abuse

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

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

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.
Note: ZENNNN provides batch APIs for imports, so there should be no need for this. Throttled calls are typically acceptable at a rate of 1 call/second,

with no parallel calls. Exceptions may be authorized on a case-by-case basis — please contact us via support@zennnn.com if you think you need one.

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, such as email bombs.

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

Attacking
Using the ZENNNN Cloud services to attack, crawl or otherwise impact the availability or security of third-party systems.

Abusive registrations
Using automated tools to repeatedly register or subscribe to ZENNNN Cloud services, or registering or subscribing with fake credentials, or under the name of someone else without their permission.