IP Transit

Acceptable Use Policy (AUP)

1. **Introduction** 3
2. **Legal and Compliant Use** 3
3. **Specific Prohibitions** 4
5. **Monitoring and Enforcement** 7
6. **Reporting Violations** 7
7. **Modifications to the AUP** 8
8. **Consequences of Violations** 8
10. **Contact and Further Information** 8

1. Introduction

This Acceptable Use Policy (hereinafter referred to as "AUP") defines the rules and expected behaviors of customers and end-users of the IP transit services provided by Orange Wholesale International (hereinafter referred to as "OWI").

This AUP is designed to ensure the security, reliability, and compliance of the services offered by OWI. By using OWI services, you agree to read and comply with this AUP.

2. Legal and Compliant Use

Customers commit to using OWI's services solely for lawful activities and in compliance with applicable laws and regulations, including, without limitation, data protection laws, intellectual property laws, and cybercrime regulations.

Customers must ensure that their use of the services does not infringe upon the rights of third parties.

Customer must not use the service in a manner that interferes with, disrupts, or causes an excessive or disproportionate load on Orange or its suppliers' infrastructure.

Customer must not engage in activities, whether lawful or unlawful, that Orange determines to be harmful to its subscribers, operations, reputation, goodwill, or customer relations.

Customer agrees and acknowledges that the violation of this AUP by his subscribers, end-users, customers and any third party who gained access to network through the customer, shall be deemed to be a violation by himself of the AUP.

Customer is solely responsible for the content of any postings, data, or transmissions using the services, or any other use of the services by his subscribers, end-users, customers and any third party who gained access to network. Customer shall not facilitate any violation of this AUP.

3. Specific Prohibitions

Customers are strictly prohibited from using OWI's services to transmit or distribute content that is not in compliance with applicable laws and regulations.

Customer shall cooperate fully with OWI in the enforcement of this AUP.

Customer shall implement appropriate measures to prevent the transmission of illegal content through the networks and shall take all necessary steps to ensure that their infrastructure is not used to facilitate prohibited activities.

Customer shall not:

- Participate in prohibited Activities related to Malware and Cyberattacks such as:

Creation or Distribution: Developing, distributing, or transmitting malware or viruses.

Exploitation: Exploiting system vulnerabilities without authorization, including the use of zero-day exploits.

Unauthorized Access: Gaining or attempting to gain unauthorized access to networks, systems, or data.

Service Interference: Interfering with service to any user, host, or network, including DoS and DDoS attacks.

Information Theft: Stealing, or attempting to steal, sensitive personal or corporate information.

Resource Misuse: Using a service provider's resources to engage in the creation or distribution of malware.

Monitoring: Executing any form of network monitoring, that could intercept data not intended for the customer.

- Spread Viruses and Malwares such as:

Viruses: Malicious software that attaches itself to clean files and spreads throughout a computer system, corrupting files, and hindering performance.

Worms: Standalone malware that replicates itself to spread to other computers, often exploiting vulnerabilities in network services.

Trojan Horses: Malicious programs that disguise themselves as legitimate software. Trojans can create backdoors, allowing unauthorized access to the affected system.

Spyware: Software that secretly monitors user activity and collects personal information without consent, often for advertising purposes.

Adware: Often unwanted software designed to throw advertisements up on your screen, most often within a web browser.

Ransomware: Malware that encrypts a user's files and demands payment in exchange for the decryption key.

Keyloggers: Spyware that records keystrokes to capture sensitive information such as passwords and credit card numbers.

- Participate in any type or allow cyberattacks such as:

Denial-of-Service (DoS) Attacks: Overwhelming a system or network with traffic to render it unavailable to its intended users.

Distributed Denial-of-Service (DDoS) Attacks: Similar to DoS but originating from multiple sources, making it harder to stop.

Man-in-the-Middle (MitM) Attacks: Interception and alteration of communication between two parties without their knowledge.

Phishing: Deceptive communications, often via email, that trick users into providing sensitive information.

Spear Phishing: A more targeted form of phishing where attackers personalize messages to deceive specific individuals.

SQL Injection: Inserting malicious SQL queries into input fields to manipulate a website's database and access unauthorized information.

Cross-Site Scripting (XSS): Injecting malicious scripts into webpages viewed by other users to bypass access controls.

Session Hijacking: Exploiting a valid computer session to gain unauthorized access to information or services in a computer system.

Credential Reuse: Using stolen account credentials on multiple websites, exploiting users who use the same password across various services.

Zero-Day Exploits: Attacks that target software vulnerabilities unknown to the vendor or for which no security fix has been released.

Drive-By Downloads: Unintentional download of malicious code to a user's system when visiting a compromised website, without any action by the user.

Malvertising: Use of online advertising to distribute malware with little to no user interaction required.

- Send unsolicited mass communications, including:

Spam: Also known as junk mail, spam refers to unsolicited bulk messages, typically sent for advertising or marketing purposes. Spam can be distributed via email, instant messaging, text messages (SMS), social media, forums, and other digital communication platforms.

Bulk Email: Large-scale email campaigns sent to numerous recipients at once, where the recipients have not explicitly agreed to receive such emails.

Mailbombing: Sending a massive volume of emails to a single address or server with the intent to overwhelm the recipient's email system.

Unsolicited Commercial Email (UCE): Email messages that are primarily commercial in nature and are sent to recipients without their consent.

Unsolicited Bulk Email (UBE): Similar to spam, UBE refers to emails sent in large quantities to multiple recipients who have not given permission to be contacted.

Chain Letters: Messages that encourage recipients to copy and forward the message to multiple contacts, often with promises of good luck or threats of bad luck if the chain is broken, or other types of pyramid schemes.

Phishing: Fraudulent attempts to acquire sensitive information by masquerading as a trustworthy entity in electronic communication. Phishing often involves unsolicited requests for personal details, login credentials, or financial information.

Spoofing and Packet Spoofing: The creation of emails or other communications with a forged sender address, often used in phishing attacks to make the message appear as if it comes from a legitimate source.

Snowballing: Like chain letters, snowballing involves sending messages that request recipients to forward the message to as many people as possible.

Unsolicited Notifications: Alerts or notifications sent to users without their prior consent, which can include push notifications from apps or browser notifications.

Unsolicited Text Messages: Text messages sent to mobile devices without the recipient's consent, often for promotional or marketing purposes.

It is not allowed to use IP Transit services to send or distribute:

Illegal Content: Any information, data, or material that violates applicable laws or regulations. This includes content related to illegal activities, such as the distribution of controlled substances, child exploitation, or pirated software.

Defamatory Content: Material that damages the reputation of an individual or entity by making false and harmful statements.

Threatening Content: Communication that implies or expresses an intention to inflict pain, injury, damage, or other hostile actions on someone.

Abusive Content: Material that is harsh, cruel, or offensive, and can include harassment, bullying, or other forms of mistreatment.

Hateful Content: Material that promotes hatred, discrimination, or violence against individuals or groups based on attributes such as race, religion, ethnicity, sexual orientation, disability, or gender.

This list is not exhaustive, and each action legality shall be defined accordingly with the applicable laws.

4. Security and Privacy

Customers are responsible for the security and confidentiality of their own systems and data.

They must implement appropriate security measures to prevent unauthorized access or data theft.

5. Monitoring and Enforcement

Customers acknowledge that OWI cannot select, modify, monitor nor censor the information transmitted over the Internet.

Therefore, OWI makes no guarantee regarding, and assume no liability for, the security and integrity of any data or information a customer, by his subscribers, end-users of customer and any third party who gained access to network through the customer transmits via the service or over the Internet.

6. Reporting Violations

Customers must immediately report to OWI any use of the services they suspect to be in violation of this AUP. Violations can be reported to the following email address: aup5511.support@orange.com

7. Modifications to the AUP

OWI reserves the right to modify this AUP at any time to reflect legal, technological, or commercial developments. Changes will be effective upon posting on OWI's website.

8. Consequences of Violations

Violations of this AUP may result in sanctions, including the suspension or termination of service contract and/or services, and may expose customers to civil or criminal liabilities.

Customers agree to indemnify and hold OWI harmless from any liability in case of claims or damages resulting from customers, customer's subscribers, end-users of customers or any third-party that gains access to the Service through customer use of the services in violation of this AUP or any applicable law.

10. Contact and Further Information

For any questions or requests for additional information regarding this AUP, please contact OWI at the following address: aup5511.support@orange.com