Xalient Acceptable Use Policy

1. Introduction

1.1. This acceptable use policy (**"AUP"**) outlines the principles that govern use of the systems, services and equipment (if any) provided by Xalient Holdings Limited, Xalient Inc., Integral Partners LLC, or their respective third parties in connection with the services we provide to you.
1.2. "User(s)" or "you" means customers or anyone else who uses or accesses our services or any services provided by a third party on our behalf as part of the services we provide to you ("services").
1.3. We reserve the right to amend, modify or substitute this AUP at any time. Your continued use of any services provided under your agreement after any such amendment, modification or substitution constitutes your acceptance of any new AUP. Any changes to the AUP will be posted on our website at www.xalient.com

2. Violations of the AUP

2.1. We reserve the right to investigate incidents involving suspected violations of this AUP. Such investigations may include gathering information from the User involved and the complaining party (if any) and examination of material on our servers, networks, third party networks or any other equipment associated with the services provided under your agreement.
2.2. We will take action if you abuse our services and/or breach this AUP. This may include, but not limited to:
(a) restriction of your access to all or any part of any service provided under your agreement (with or without notice); or
(b) suspension or termination of any service under your agreement (with or without notice).
2.3. If we impose a suspension, then this may be lifted at our discretion upon receipt of a formal written undertaking from you not to commit any future relevant abuse.
2.4 If you are a reseller of our services it is your responsibility to ensure end users comply with the terms of this AUP.

3. Illegal Use

3.1. Our services may be used only for lawful purposes.
3.2. As the User of the services you agree to comply with all applicable laws, statutes and regulations of any relevant jurisdiction applicable to the use of the services.
3.3. If your use of the services is under investigation by relevant authorities, we reserve the right to suspend the services for the duration of the investigation.

4. Security

4.1 Violations of system or network security are prohibited and may result in criminal and civil liability. We will investigate incidents involving such violations and may involve and will cooperate with law enforcement agencies if a criminal violation is suspected.
4.2 We reserve the right to suspend or disconnect your services without notice if there is a violation of the system or network security.
4.3 Unless we have agreed otherwise in our agreement with you the security of the services used by you is your responsibility. We are not responsible for the consequences of your failure to employ adequate security measures (e.g. lost or corrupted files, identity theft, fraud).

Examples of system or network violations include, but not limited to, the following:

- Unauthorized access to or use of computers, data, systems, accounts or networks, including any attempt to probe, scan, or test the vulnerability of a system or network or an attempt to penetrate security measures of another individual's system (known as 'hacking').

- Unauthorized monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network.
- Interference with the services to any user, host or network including, without limitation, mail-bombing, flood, deliberate attempts to overload a system and broadcast attacks.
- Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting or otherwise engaging in any monitoring or interception of data not intended for the User without authorization is prohibited.
- Engaging in or permitting any network or hosting activity that results in the blacklisting or other blockage of IP space is prohibited.
- Also, attempting to circumvent client authentication or security of any hosts, network, or account ('cracking') without authorization is prohibited. Simulating communications ("phishing") from and/or to a website or other service of another entity in order to collect identity information, authentication credentials, or other information from the legitimate users of that entity's service is prohibited.
- Exporting encryption software over the Internet or otherwise in violation of ITAR, to points outside the United States is prohibited.
- Using malware, DNS cache poisoning or other means ("pharming") to redirect a user to a website or other service that simulates a service offered by a legitimate entity in order to collect identity information, authentication credentials, or other information from the legitimate users of that entity's service is prohibited.
- Activities that disrupt the use of or interfere with the ability of others to effectively use any network, system, services, or equipment by utilizing programs, scripts, or commands to abuse a website (i.e., DDOS, SYN Floods or similar attacks).
- Furnishing false data including fraudulent use of credit card numbers.

5. Content/email

5.1. You are prohibited from storing, distributing, transmitting or causing to be published any "prohibited material" through your use of the services, including for example your use of the services to send emails, post on online forums and use social media. What constitutes "prohibited material" shall be determined by us (acting in our sole discretion). Prohibited material includes (without limitation):

5.1.1. material that is threatening, harassing, invasive of privacy, discriminatory, defamatory, racist, obscene, indecent, offensive, abusive, harmful or malicious;

5.1.2. material that infringes or breaches any third party's intellectual property rights (which shall include, but not be limited to copyright, trademarks, design rights, trade secrets, patents, moral rights, paternity rights and performance rights) – this includes the use, distribution and/or copying of any material without the express consent of the owner;

5.1.3. material that is in violation of any applicable laws, statutes or regulations of any relevant jurisdiction applicable to the use of the services; and

5.1.4. programs containing viruses, worms, trojan horses, malware (malicious software), hoaxes or any tools designed to compromise the security of Internet users, websites and/or systems. However, you may pass samples of malware in a safe manner to appropriate agencies for the purpose of combating its spread.

5.2. For the avoidance of doubt, the storage or distribution of "pirated" software, or any other materials that are not expressly licensed to the User, will constitute a violation of this AUP.

5.3. At our sole discretion (and without prejudice to any of our other rights pursuant to this AUP), we reserve the right to remove or block any material from any server under our control. In addition to any other action we may take, we reserve the right to notify relevant authorities, regulators and/or other third parties of the use, storage, distribution, transmission, retransmission or publication of

prohibited material (and/or any other materials the dealing with or use of which may constitute unlawful conduct by Users).

6. Sending high volume of traffic to particular autonomous system

If the traffic to and from a particular ASN exceeds 10%, or such other percentage we may have agreed with you, of your monthly Committed Data Rate (CDR) then we make no guarantee of performance towards packet loss and/or latency to and from that ASN. This also applies to "Transit" Autonomous systems which are used to reach the end user destinations.

7. Additional terms and conditions

This AUP shall apply to all agreements or statements of work agreed between us.