Acceptable Use Policy

1) General

a) This Acceptable Use Policy (**Policy**) sets out the rules that apply to Customer's use of the Services supplied by Megaport (USA) Inc., or one of its Affiliates (**Megaport**) on the Megaport network.

b) The purpose of this Policy is to ensure that Customers use of the Services is lawful and does not interfere with the network or anyone else who uses Megaport Services or the internet.

c) Each Customer is responsible for ensuring that use of the Services and Customer's Megaportal account complies with this Policy, even if that use occurred without Customer's authority. If Customer fails to comply with this Policy, Megaport may restrict, suspend or terminate the Services.

d) Customer agrees that while the contractual relationship with Megaport is governed by the law specified in the Customer's service agreement with Megaport, other national or international laws may be applicable, in respect of Megaport's supply of the Services. Infringement of those laws constitutes a breach of this Policy and Megaport will be permitted to take action in response to such a breach in accordance with this Policy.

e) Capitalised words used in this Policy have the meaning given to them in Customer's service agreement, unless defined in this Policy or the context requires otherwise.

2) Changes to this Policy

Megaport can make changes to this Policy at any time by posting the updated policy at www.megaport.com/legal and giving Customer notice in accordance with Customer's service agreement. Customer is responsible for checking this website regularly for updates. Any changes to the Policy will take effect in accordance with the terms of Customer's service agreement. If there is any inconsistency between Customer's service agreement and this Policy, this Policy will apply.

3) Using the Services

a) In using the Services, Customer will act responsibly and use the Services for lawful purposes only. Customer must not use, attempt to use or allow the Services to be used to store, send, distribute or otherwise make available any content or material that:

b) is prohibited by or breaches any applicable laws and any other order, regulation, standard, code of practice or guideline or which is likely to be offensive or obscene to a reasonable person;

    i) is confidential or subject to copyright or third-party intellectual property rights (unless Customer has a lawful right to do so);

    ii) defames, harasses, threatens or abuses anyone or violates their privacy or misuses their personal data; or

    iii) is otherwise illegal, fraudulent or likely to give rise to civil liability or criminal prosecution.

c) Customer must not do anything that endangers any person or the integrity, security or performance of Megaport's network, systems or equipment or that of anyone else. Customer must not use, attempt to use or allow the Services to be used to:

    i) obtain or attempt to obtain unauthorised access to Megaport's or anyone else's equipment, systems, networks or personal data for any purpose;

    ii) store, send or distribute any viruses or other harmful programs, codes or malicious software;

iii) store, send or distribute tools designed for compromising security including, but not limited to, password guessing programs, cracking tools, packet sniffers or network probing tools;

iv) hinder, restrict or interfere with the normal operation of Megaport's systems, network or equipment or that of anyone else;

v) conduct any action that is not related to the procurement of the Services supplied by Megaport;

vi) access or search any part of the Services, or data relating to Services or other Megaport Customers, by any means other than Megaport's publicly supported interfaces (for example, not engage in "scraping"); or

vii) hinder, restrict or interfere with the ability of other people or systems to use Megaport's Services or any services provided by anyone else.

d) Customer must comply with applicable laws in respect of the sending of unsolicited messages or spam and in particular must not:

i) send, relay or distribute any unlawful unsolicited commercial electronic messages;

ii) send messages that do not include accurate sender information and do not contain an unsubscribe facility; or

iii) use or distribute any software designed to harvest email addresses.

e) In using the Services, Customer must not:

i) obscure, alter or delete the source of message that Customer sends, or forge message headers;

ii) send or distribute material with the intent of overloading the network or system or that of anyone else (e.g. 'mail bombing'); or

iii) make fraudulent offers or promote any type of financial scam (e.g. 'pyramid schemes', 'Ponzi schemes').

f) Customer must not do anything to authorise, aid, abet, encourage or incite any person to do or attempt to do any of the acts or engage in any conduct that is prohibited by this Policy.

g) Customer must not store, send or distribute, attempt to store, share or distribute or otherwise make available any of the Service content, material or data to any third party.

h) This Policy provides examples of restricted behaviour but does not list all restricted behaviours. Megaport retains full discretion to decide whether a Customer's use violates the Policy.

4) **Security**

Customer is responsible for implementing and maintaining the security of its use of the Services, including protecting Customer's Megaportal account, Customer's devices, equipment, systems and its own network against unauthorised access. More specifically, note that although Megaport secures its network, Customer is still responsible for securing the data that the Customer chooses to transmit through Megaport's network and should encrypt its data. Megaport won't be liable to anyone in any way for any losses or harm suffered to the extent caused (directly or indirectly) by Customer's failure to encrypt its data.

5) **Access to Internet content**

a) Customer is responsible for determining the content and information Customer chooses to access on the Internet when using the Services.

b) It is Customer's responsibility to take all steps Customer considers necessary (including the use of filtering programs) to prevent access to offensive or obscene content on the Internet by children or minors who Customer allows to use the Services.

c) Customer must not use or attempt to use the Services to make inappropriate contact with children or minors who are not otherwise known to Customer.

6) **Content publishing**

a) Customer is responsible for any content Customer publishes on publishing mediums (eg. websites, email, online forums) accessed via the Services.

b) Customer must not use the Services to send or distribute any content that is prohibited, deemed obscene or offensive or otherwise unlawful under any applicable law. Customer must take appropriate steps to ensure that minors do not access or receive any content Customer has published that may be inappropriate for them.

c) Customer must clearly identify any content Customer publishes using the Services in accordance with the applicable codes of practice and guidelines relating to media or broadcasting or any other industry code or content standard that applies to Customer's use or distribution of that content.

d) Subject to clause 9(b), if Customer fails to comply with the requirements in this section 6, Megaport may suspend or terminate the Services on reasonable notice, provided that Megaport may immediately suspend Services without notice if Customer materially fails to comply with this Acceptable Use Policy.

e) Customer warrants that the content Customer copies, stores, sends, distributes or otherwise makes available using the Services complies with this Policy including applicable laws in respect of data protection and privacy. Customer authorises Megaport (or Megaport's agents) to copy, store, send, distribute or otherwise make available such content as necessary for Megaport to deliver the content.

7) **Megaport's compliance obligations under applicable laws**

Customer acknowledges that:

a) copyright owners or their agents may direct Megaport to remove copyright materials from the network or systems or to prevent people from accessing those materials;

b) Megaport may provide information (including personal information) about Customers and their use of the Services to copyright owners and their agents;

c) appropriate law enforcement authorities or agencies may direct Megaport to remove from the network and servers any content which is classified, or likely to be classified as prohibited, obscene or indecent content;

d) Megaport may take steps to minimise the amount of unsolicited electronic messages; and

e) Megaport may take steps to comply with any such directions or requirements of law enforcement authorities or agencies, without notice to Customer.

8) **Capacity**

a) Without limiting Megaport's other rights, if the load on one of Customer's Ports reaches or exceeds the maximum allowed capacity on that Port (as stated in Customer's Order) for:

   i) a period of two consecutive months; or

   ii) any three months within a period of six months,

   Megaport may, by notice, request that Customer decrease the load on that Port, increase the capacity of that Port or order another Port within 30 days from the date of the notice.

b) Megaport's Network Operations Centre will monitor utilisation of:

    i) Cloud Service Provider (**CSP**) ports and all Customer VXCs for Congestion Events; and

    ii) Customer ports and VXCs between customer ports or Cloud Service Providers (CSP) for Network Congestions Events.

c) Any Customer VXC deemed to be causing a Congestion Event or a Network Congestion Event will be immediately reduced by the Megaport Network Operations Centre to a speed that alleviates the congestion. The Customer VXC speed reduction will remain in place until:

    i) the Congestion Event or the Network Congestion Event is deemed to have ended; and

    ii) for a Congestion Event, the CSP port utilisation falls below 95% and remains uncongested over a continuous 15 minute period; or

    iii) for a Network Congestion Event, the network circuit utilisation falls below 95%, the service returns to an acceptable throughput and remains uncongested over a continuous 15 minute period.

For the purposes of this Policy, a Congestion Event is defined as the CSP port utilisation exceeding 95% and a Network Congestion Event is defined as the network circuit utilisation exceeding 95% of the total available capacity and/or causing degradation of service for other customers.

d) Megaport Service Desk will advise Customers impacted by the VXC speed reduction via email at the time of the Congestion Event and at the completion of the Congestion Event. The customer is responsible for restoring the VXC speed after any reduction made in accordance with clause 8(c) above.

9) Breach of this Policy

a) If Megaport reasonably believes that Customer, or someone with access to the Services, is using the Services in a way that breaches this Policy, Megaport may take any responsive action Megaport considers appropriate. This may include the blocking or removal of any data or content or the suspension or termination of the Services. In the case of blocking or removal of data or content, the Customer shall have the right to terminate the Agreement under the Global Services Agreement.

b) If practicable, Megaport will first take reasonable steps to contact Customer and give the Customer an opportunity to rectify a breach or suspected breach of this Policy within a reasonable period. What is a reasonable period will depend on the severity of the breach and it may be reasonable (e.g. if the breach is serious or continuing) to take responsive action immediately without notice. Before Megaport terminates the Services, Megaport will provide Customer with notice and an opportunity to rectify the breach in accordance with Customer's service agreement.

c) Megaport's rights to suspend or terminate any Service will be exercised subject to any applicable laws in place in the jurisdiction in which the Services are delivered.

10) API Usage

a) Megaport may monitor the use of the APIs to manage experience and ensure Customer API integrations are compliant with Megaport's quotas. Exceeding the quotas either by accident or deliberately may result in a temporary suspension of the ability to make API requests to Megaport systems.

b) General API requests collect Megaport provisioning information or service metrics.

c) Service Updates are API requests that make a change to network elements and service configuration, resulting in a change to service parameters and impacting billing.

API Request Category	Quota

General API requests	• Limit of 500 requests in a rolling 5 minute period per IP address
Service Update requests	• No more than one update every 5 minutes and a maximum of 100 updates per month (per service)