Acceptable Use Policy (AUP)

An explanation of the appropriate use of Partnerize services

Author:

1 Introduction

At Partnerize, our mission is to improve the effectiveness and sophistication of partnership by applying data and advanced technology to every aspect of Partner Management but that shouldn't be at the expense of other people's safety and rights. That's why we have a few rules on how our services can and can't be used. This policy explains them, what we might do if you break them, and what to do if you've got any concerns.

It applies to all of our services and also applies to different ways you might use our services. By using our services, you agree to follow and comply with our acceptable use policy. We might update it from time-to-time but when we do we will let you know. The AUP is hosted on partnerize.com and by continuing to use our services after we update this policy, you're accepting the new terms.

2 Purpose

This Acceptable Use Policy is intended to provide a framework for the appropriate use of Partnerize services.

3 Policy

3.1 Prohibited Actions

You agree not to misuse Partnerize services or to help anyone else to do so. For example, you must not do any of the following in connection with the services:

- actions that restrict or inhibit anyone - whether a customer of Partnerize or otherwise - in the use of Partnerize products and services, or that generate excessive network traffic;
- causing or attempting to cause security breaches or disruptions of Partnerize services. Security breach examples include but are not limited to accessing data of which the customer is not an intended recipient or logging into a server or account that the customer is not expressly authorized to access. Examples of disruption to Partnerize services include but are not limited to port scans, flood pings, packet spoofing and forged routing information;
- probing, scanning or testing for vulnerabilities on any Partnerize system or network;
- introduction of malicious programs into the Partnerize platform;
- intentionally or unintentionally interfering with or denying services (denial of service attack);
- send unsolicited communications, promotions or advertisements, or spam via the Partnerize platform.

3.2 Illegal Activities

The following activities are considered illegal; therefore, they are also prohibited:

- promoting or advancing criminal activities, including terrorism, human trafficking or modern day slavery;

- hacking Partnerize computers, systems or networks whether they're ours or someone else's;
- sending or uploading any material containing any viruses or other harmful programs or code
- designed to adversely affect the operation of any software or hardware;
- infringing copyright or other intellectual property rights;
- impersonating someone else, or otherwise misrepresenting who you are or falsely claiming to represent Partnerize in communications with others;
- using the system in any way which would breach any applicable local, national or international law or regulation.

3.3 Our Rights

If we have reason to believe that:

- any part of our Acceptable Use Policy has been breached; and/or
- fraudulent data or information is being entered, stored or sent by or into the Partnerize system; (jointly a “Breach”)

we have the right to take any or all of the following actions:

- require you to:
    - initiate an internal investigation of the suspected Breach;
    - keep us informed of the progress and findings of this investigation as reasonably
    - required to remediate any such Breach; and/or
    - cooperate with us as reasonably required to resolve the suspected Breach as soon as
    - reasonably practicable.
- require you to assign personnel to resolve the suspected Breach promptly, or more expeditiously, taking into account the severity of the Breach and the likely impact to the working on the Partnerize system;
- immediately restrict any access to any suspected or actual illegal material or data;
- limit, suspend or block access to any or all of our services (including without notice where
- reasonably required);
- suspend or terminate your access to some or all of the services;
- take legal action against you.

In serious cases, we can report you to the police or other law enforcement agency where we consider this reasonably required.

We exclude our liability for all action we may take in response to breaches of this Acceptable Use Policy. The actions we take are not limited to those described above and we may take any other action we deem reasonably appropriate, with or without prior written notice to you.

3.4 ContactUs

If you are unsure of whether any contemplated use or action is permitted, please contact Partnerize at techops-support@partnerize.com.

3.5 Compliance

Compliance with this policy is mandatory and the consequences of a breach have been outlined in the section titled “Our Rights”.

3.6 Review and Revision

This policy will be reviewed annually by Partnerize.

4 Compliance

It is mandatory for all staff to comply with this policy. Any violation or suspected violation of this policy by staff will be investigated and may be treated as a disciplinary offence and dealt with in accordance with the staff handbook.

5 Document Control

Document Control	
Author	Leigh Carlin
Owner	SVP of Technical Operations
Version Number	1.1
Date	08/03/22

6 Summary of Changes

Version Number	Version Date	Author	Summary of Changes
0.1	23/07/2020	Leigh Carlin	Initial draft
1.0	07/10/2020	Jennifer Kilmartin	Reviewed and approved
1.1	08/03/2022	Jennifer Kilmartin	New logo and format

7 Approvals

Version Number	Approval Date	Approved By
1.0	07/10/2020	Paul Fellows, Chief Operating Officer

8 Roles and Responsibilities

Responsible	Platform Support Team
Accountable	Platform Support Team
Consulted	Information Security & Compliance Team
Informed	Staff members

9 Related Documentation

Document Name