Acceptable Use Policy

Date distributed:

4th June 2020

ACCEPTABLE USE POLICY

1. Definitions

AUP means this Acceptable Use Policy;

Client means the entity or person that uses the Services;

Customer Care Plan means Micron21's paid managed service plans;

Intellectual Property Rights means all present and future intellectual and industrial property rights conferred by statute, at common law or in equity and wherever existing, including:

(a) patents, designs, copyright, rights in circuit layouts, plant breeder's rights, trade marks, know how, brand names, domain names, inventions, product names, trade secrets, confidential information and any other rights subsisting in the results of intellectual effort in any field, whether or not registered or capable of registration;

(b) any application or right to apply for registration of any of these rights;

(c) any registration of any of those rights or any registration of any application referred to in paragraph (b); and

(d) all renewals and extensions of these rights;

MSA means the Master Services Agreement entered into by Micron21 and the Client;

Micron21 means Micron21 Data Centre Pty Ltd;

Personal Information means any information or opinion about a natural person (whether or not true), as defined in the Privacy Act, which the Client deals with, in connection with performing its obligations under this AUP;

Privacy Act means the Privacy Act 1988 (Cth);

Privacy Law means the Privacy Act (including the Australian Privacy Principles under the Privacy Act), and any other privacy or general legislation which binds the Client, and which relates to the protection of Personal Information;

Sensitive Information means 'Sensitive Information' as defined in the Privacy Act;

Services means the services provided by Micron21 to the Client and includes any support services or any other type of service provided by Micron21 to the Client as set out in the Statement of Work;

Statement of Work means a written statement (including any attachments) for the provision of the Services by Micron21 to the Client pursuant to the terms in the MSA;

SPAM Act means the Spam Act 2003 (Cth);

Technologies includes, but is not limited to, IT equipment and peripherals, electronic communications, operating systems, user accounts, internet services, mobile phones, portable devices, telephones, internet service applications and software, network services and networks, databases, files and any information stored thereon or therein which is owned, leased, or managed by Micron21.

2. General Obligations

2.1 The obligations set out in this AUP are in addition to the obligations set out in the MSA.

2.2 The Client acknowledges that it is solely responsible for all content, materials, and activities in relation to the Client's use of the Services.

2.3 The Client must not undertake anything that violates any applicable local, state, federal or international laws, standards or codes of conduct in relation to the Client's use of the Services.

2.4 The Client must ensure that any of the Client's end users or customers, that directly or indirectly use the Services, also comply with this AUP.

3. Unacceptable Use and Prohibited Activities

3.1 The Client must use the Services in a lawful, ethical and professional manner.

3.2 Under no circumstances shall any of the Services be utilised by the Client to:

(a) publish, distribute, promote, or link to other websites that store child pornography or any content that exploits or is harmful to children;

(b) place another person's well-being, safety or security at risk;

(c) interfere with an investigation of any law enforcement agency;

(d) place at risk or compromise national security;

(e) engage in activities related to terrorism or a terrorist organisation;

(f) make or publish derogatory, inflammatory, or discriminatory comments or content that is deemed as hate speech;

(g) disclose Personal Information or Sensitive Information of another in breach of the Privacy Act;

(h) infringe the Intellectual Property Rights of another person, business or entity;

(i) host or link to any kind of proxy server or other traffic relaying programs;

(j) host, promote or link to any form of fraudulent activity or activity intended to deceive others;

(k) host, promote or link to other websites to perform multi-level marketing, ponzi/pyramid schemes, high-yield interest programs, money laundering or similar activities;

(l) engage in phishing or identity theft related activities;

(m) sell or otherwise provide goods or services that are illegal, dangerous, or without the required permits to do so;

(n) knowingly or deliberately introduce or distribute malicious programs including, but not limited to, viruses, trojans, ransomware, malware, malicious code or spyware;

(o) circumvent Micron21's virus protection, security measures, access and controls;

(p) engage in activities intended to disrupt the Services and the Technologies or that of other Micron21 clients;

(q) attempt or to gain access to the Technologies without permission, or use tools and techniques designed to probe for vulnerabilities in the Technologies;

(r) access restricted information or data without authorisation;

(s) undertake activities that is detrimental to Micron21's professional reputation; and

(t) use the Services in anyway deemed unacceptable by Micron21.

4. Bulk Emails and SPAM

4.1 The Client must not use the Services to:

(a) send spam or bulk unsolicited messages, or the sending, or commissioning the transmission of commercial e-mail that does not comply with the SPAM Act;

(b) use or distribute software designed to collect or harvest email addresses without consent;

(c) host, support or otherwise engage with spammers in relation to the Services; or

(d) cause any of Micron21's internet protocol (**IP**) ranges or IP addresses to become listed by any online SPAM database or cause to impede the delivery of legitimate emails.

5. Excessive Use

5.1 Micron21 provides the Services for the reasonable use by the Client which includes, from time to time and for limited durations, increased activity or resource demands placed on the Technologies and the Services.

5.2 The Client must not:

(a) exceed and sustain 75% CPU utilisation for more than 15 minutes;

(b) utilise bandwidth outside the following percentage use, on average, within a calendar month: 80% domestic peering, 10% domestic telecommunication carriers and 10% international telecommunication carriers;

(c) perform any disk input/output (**IO**) activity that sustains excessive load as determined by Micron21 and communicated to the Client from time to time;

(d) exceed the allocated support hours on a Customer Care Plan in aggregate for any 12month period from the plan's commencement date or exceed the support hours set out in the Client's Customer Care Plan for two consecutive calendar months;

(e) exceed two support hours or ten support requests in a calendar month on Micron21's complimentary 24/7 support plan, excluding issues that are related to the delivery or availability of the Services or Technologies;

(f) run or use resource-intensive programs or services which adversely affects other Micron21 clients or the Technologies. This includes, but is not limited to, torrents,

peer-to-peer (P2P) networks, crypto-currency mining, scanning or benchmarking software; or

(g) impact the quality or operations of the Technologies for the use of other Micron21 clients.

5.3 Micron21 reserves the right to:

(a) terminate or suspend the Statement of Work; or

(b) restrict the provision of the Services,

should the Client engage in any of the activities set out in clause 5.2 above, or any other activity reasonably determined by Micron21 to have an adverse effect on the Services or the Technologies.

6. Client Equipment

6.1 Clients that supply their own equipment to be hosted or co-located at Micron21's facility must ensure that this equipment:

(a) does not present a safety or health risk to Micron21 personnel;

(b) is free from defect, or such defects are remedied within a reasonable period of time;

(c) conforms to the manufacturer's specifications and operates within the manufacturer's guidelines; and

(d) does not adversely impact the Technologies or the provision of the Services.

7. Security

7.1 The Client is solely responsible for any misuse of the Services, even if the inappropriate activity was committed by another person under the Client's account. The Client is responsible for taking all necessary measures to ensure that others do not gain unauthorised access to the Services.

7.2 The Client will be solely responsible for any breach of this AUP as a result of the activities, content or material of the Client's end users or customers, when using the Services.

7.3 The Client must not use its account to breach the security of another account of Micron21's clients or attempt to gain unauthorized access to another network or server.

7.4 The Client agrees to keep all software up to date with the latest stable release, with the exception of software managed by Micron21 under a Customer Care Plan.

7.5 The Client agrees to keep safe any usernames and passwords in a secure location;

7.6 Where the Client has chosen not to purchase or perform backups as part of the Services, Micron21 is not liable to the Client for any data breach, data loss or ransom to retrieve data that the Client may experience during the provision of the Services.

8. Remedy

8.1 If Micron21 reasonably believes that the Client has breached or is about to breach this AUP and/or a Statement of Work, Micron21 may take actions in order to prevent or stop the breach or limit any adverse impacts on the Services. These actions may include:

(a) temporary or permanent removal of content or the ability to publish content;

(b) filter, limit, block or alter the Client's access to electronic communications and the Services;

(c) terminate or suspend all or any part of the Services set out in the Statement of Work;

(d) cooperate with any law enforcement authorities in relation to alleged or suspected illegal activity;

(e) cooperate with any network providers in relation to any misuse of a telecommunication network or service;

(f) assist the requests of any government agency, regulator or third-party rights holder;

(g) immediately restrict or deny the Client access to Micron21's, facility, premises, the Services, or the Technologies; and

(h) any other action reasonably determined by Micron21.

8.2 The Client is solely liable for any fees or charges incurred by Micron21 to third party providers for the removal of any restrictions that have been placed on Micron21 or the Services as a result of breaching this AUP.

8.3 The Client will not be entitled to any refunds if found in breach of this AUP or for any periods during which the Services are terminated, suspended or restricted.

9. AUP Revisions

9.1 Micron21 reserves the right to revise, amend or modify this AUP at any time (**AUP Revisions**).

9.2 AUP Revisions will come into effect when and as published on Micron21's website.

9.3 The Client agrees to use the Services in compliance with AUP Revisions.

9.4 Notwithstanding clause 9.3, the Client may terminate a Statement of Work if the Client reasonably believes that the AUP Revisions:

(a) would cause a significant imbalance to the Client's rights and obligations under a Statement of Work;

(b) are not reasonably necessary to protect Micron21, the Services or the Technologies; and

(c) would cause detriment (financial or otherwise) to the Client.

10. Conflict with MSA

To the extent that the terms of this AUP are inconsistent or conflict with the terms of the MSA, the terms of the MSA shall prevail.

11. Reporting Violations

If the Client determines that a violation of this AUP has occurred, the Client must contact Micron21 either via email support@micron21.com or call 1300 769 972.