Cyxtera

Acceptable Use Policy

Last Updated: December 19, 2018

I. Introduction and Applicability of Acceptable Use Policy

Cyxtera Data Centers, Inc. and its subsidiaries, parent companies, and affiliates (collectively "Cyxtera" or "Company" or "we") have adopted this Acceptable Use Policy ("AUP") to govern the use of their Extensible Data Center Platform (CXD) and general interconnection services (the "Services") by their customers ("Customers" or "you") and by users that have gained access to the Services through Customer accounts ("Users"). As used in this AUP, any reference to "Users" is intended to encompass, as applicable, both Customers and their Users, and any reference to "Services" is intended to encompass, as applicable, both the Services and the Cyxtera Environment and Network (as defined below). Any use of the Services by a User in violation of this AUP shall also be considered a use of the Services by Customer in violation of this AUP and any other breach by a User of this AUP shall also be considered a breach by Customer of this AUP. In the event Cyxtera has a right hereunder to terminate or suspend an individual User's right to use any or all of the Services, Cyxtera shall also have the right to terminate or suspend, as the case may be, Customer's (and all other User's) right to use such Services.

By using the Services, you acknowledge that you and your Users are responsible for compliance with this AUP, and agree to be bound by this AUP. You are responsible for violations of this AUP by any User that accesses the Services through your account. Cyxtera does not intend to control or monitor any User's experience or the content of their online communications, however, Cyxtera reserves the right to disconnect or otherwise terminate your (and all of your Users') access to the Services for usage that violates (or may violate) the AUP or that otherwise appears unlawful, harmful or offensive. This AUP applies to all aspects of the Company's Services, including any aspects of such Services across Cyxtera's network, including equipment, systems, facilities, services and products incorporated or used in such transmission network ("Cyxtera Environment and Network"). This AUP is designed to protect the Services (including the Cyxtera Environment and Network), Users, and the Internet community from improper or illegal activity across the Internet, to improve the Services and to improve Services offerings. In situations where data communications are carried across networks of other Internet Service Providers (ISPs), you and Users must also conform to the applicable acceptable use policies of such other ISPs.

The use of the Services by a Customer (and any other User accessing the Services through Customer) is subject to the terms and conditions of any agreements entered into by such Customer and Cyxtera. This AUP is incorporated into such agreements by reference. Certain Services may have additional terms and conditions, which govern in the event of any inconsistency with this AUP. Please refer to the specific products and services terms and conditions including any specification sheets as well as FAQs, and the agreements under which such products and services are being provided for further information.

If you do not wish to be bound to this AUP, you should not access, subscribe to, or otherwise use the Services or permit any Users to do any of the foregoing. Cyxtera may modify this AUP at any time, without notice to you or any of your Users. Modifications will be deemed effective immediately upon posting of the modified terms at Cyxtera's website.

II. Prohibited Uses

2.1 Illegal Activity

Users may access and use the Services for lawful purposes only. You are responsible for any transmission you or your Users send, receive, post, access, or store using the Services, including via the Cyxtera Environment and Network. Users must at all times use the Services in compliance with all applicable laws, rules and regulations. Cyxtera strictly prohibits the use of the Services for the transmission, distribution, retrieval, or storage of any information, data, or other material in violation of any applicable law or regulation (including, where applicable, any tariff or treaty). This prohibition includes, but is not limited to, the use or transmission of any data that is protected by copyright, trademark, trade secret, patent or other intellectual property right without proper authorization and the transmission of any material that constitutes an illegal threat, violates export control laws, or is obscene, defamatory, or otherwise unlawful. Some examples of unlawful conduct include:

- *Infringement*: Infringement of intellectual property rights or other proprietary rights including, without limitation, material protected by copyright, trademark, patent, trade secret or other intellectual property right. Infringement may result from the unauthorized copying, distribution and/or posting of pictures, logos, software, articles, musical works, and videos.
- *Offensive Materials*: Disseminating or posting material that is unlawful, libelous, defamatory, obscene, indecent, explicit, lewd, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, inflammatory or otherwise objectionable.
- *Export Violations*: Including, without limitation, violations of the Export Administration Act and the Export Administration Regulations administered by the Department of Commerce.

2.2 Unauthorized Access/Interference

A User may not attempt to gain unauthorized access to, or attempt to interfere with or compromise the normal functioning, operation, or security of any portion of the Services. A User may not use the Services to engage in any activities that may interfere with the ability of others to access or use the Services or the Internet. A User may not use the Services to monitor any data, information, or communications on any network or system. A User is strictly prohibited from attempting to gain access to the user accounts of other customers or users, or violating system or network security, each of which may result in criminal and civil liability. Cyxtera will investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Cyxtera may, but is under no obligation to, monitor equipment, systems and network equipment at any time for security and management purposes. Examples of prohibited unauthorized access or interference include:

- *Hacking*: Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without the express prior authorization of the owner of the system or network.
- *Interception*: Unauthorized monitoring of data or traffic on any network or system without the express prior authorization of the owner of the system or network.
- *Intentional Interference*: Interference with service to any user, host or network including, without limitation, denial-of-service attacks, mail bombing, news bombing, other flooding techniques, deliberate attempts to overload a system, and broadcast attacks.
- *Falsification of Origin or Routing Information*: Using, selling, or distributing in conjunction with the Services, any computer program designed to conceal the source or routing information of electronic mail messages in a manner that falsifies an Internet domain, header information, date or time stamp, originating e-mail address, or other identifier.
- *Avoiding System Restrictions*: Using manual or electronic means to avoid any limitations established by Company or attempting to gain unauthorized access to, alter, or destroy any information that relates to any Company customer or other end-user. Company may, but is not obligated to, take any action it deems necessary to protect the Services, its rights or the rights of its customers or third parties, or optimize or improve the Services, systems, and equipment. Users acknowledge that such action may include, without limitation, employing methods, technologies, or procedures to filter or block messages and data sent through the Services. Company may, in its sole discretion, at any time, filter "spam" or prevent "hacking," "viruses" or other potential harms without regard to any preference Users may have communicated to us.
- *Failure to Abide by Third-Party Policies*: Violating the rules, regulations, or policies that apply to any third-party network, server or computer database that a User accesses.
- *Harmful Content*: Disseminating or posting harmful content including, without limitation, viruses, Trojan horses, worms, time bombs, zombies, cancelbots or any other computer or other programming routines that may damage, interfere with, secretly intercept or seize any system, program, data or personal information.

2.3 Spoofing/Fraud

Users are prohibited from intentionally or negligently injecting false data into the Internet via the Services, for instance in the form of bad routing information (including, but not limited to, the announcing of networks owned by someone else or reserved by the Internet Assigned Numbers Authority) or incorrect DNS information.

Cyxtera

A User may not attempt to send e-mail messages or transmit any electronic communications using a name or address of someone other than such User for purposes of deception via the Services. Any attempt to impersonate someone else by altering a source IP address information or by using forged headers or other identifying information is prohibited. Any attempt to fraudulently conceal, forge, or otherwise falsify a User's identity in connection with use of the Services is also prohibited.

2.4 Unsolicited Commercial E-mail/Spamming

A User may not use the Services to transmit unsolicited commercial e-mail messages or deliberately send excessively large attachments to one recipient, or files that disrupt a server, account, newsgroup, or chat service. Any unsolicited commercial e-mail messages or a series of unsolicited commercial e-mail messages or large attachments sent to one recipient using the Services is prohibited. In addition, "spamming" or "mail-bombing" using the Services is also prohibited.

Likewise, Users are precluded from transmitting using the Services: (1) unsolicited informational announcements; (2) chain mail; (3) numerous copies of the same or substantially similar messages; (4) empty messages; or (5) messages which contain no substantive content. Use of the service of another provider to send unsolicited commercial e-mail, spam, or mail-bombs, to promote a site hosted on or connected to the Services, is similarly prohibited. Likewise, a User may not use the Services to collect responses from mass unsolicited e-mail messages, e-mail addresses, screen names, or other identifiers of others (without Company's prior written consent), a practice sometimes known as spidering or harvesting. You and your Users may not use any of Company's mail servers or another site's mail server to relay mail without the express permission of the account holder or the site.

You and your Users will not access any Usenet newsgroups via any network other than one provided through the Services. Without notice to you, and at any time, Cyxtera may add, remove, or modify Usenet newsgroups or services and may modify or restrict the bandwidth available to download content from Usenet newsgroups.

Cyxtera may, in its sole discretion, rely upon information obtained from anti-spamming organizations (including, for example and without limitation, spamhaus.org, spamcop.net, sorbs.nte, and abuse.net) as evidence that a User is an active "spam operation" for purposes of taking remedial action under this AUP.

2.5 Usenet Postings

All postings to Usenet groups must comply with that group's charter and other policies. Users are prohibited from cross-posting to unrelated news groups or to any news groups where the post does not meet that group's charter. Continued posting of off-topic messages, including commercial messages (unless specifically invited) is prohibited. Disrupting newsgroups with materials, postings or activities that are (as determined by Cyxtera in its sole discretion) frivolous, unlawful, obscene, threatening, abusive, libelous, hateful, excessive or repetitious is prohibited, unless such materials or activities are expressly allowed or encouraged under the newsgroup's name, Frequently Asked Questions, or charter.

2.6 Miscellaneous Prohibited Activities

Cyxtera prohibits Users from using the Services for any prohibited activities, including, but not limited to, the following activities:

- Intentionally transmitting files containing a computer virus or corrupted data.
- If Cyxtera has specified bandwidth limitations for your user account, use of the Services shall not be in excess of those limitations.
- Attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization, or other methods to document use of the Services.
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.

- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network.
- Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP, which includes the facilitation of the means to deliver unsolicited commercial e-mail.
- Any activity that disrupts, degrades, harms or threatens to harm the Services, including the Cyxtera Environment and Network.
- Any use of another party's electronic mail server to relay email without express permission from such other party.
- Any other inappropriate activity or abuse of the Services (as determined by Cyxtera in its sole discretion), whether or not specifically listed in this AUP, may result in suspension or termination of the User's access to or use of the Services.

2.7 <u>Complaints</u>

If Cyxtera receives complaints directly from Internet users, through Internet organizations and through other parties, Cyxtera shall not be required to determine the validity of complaints received, or of information obtained from anti-spamming organizations, before taking action under this AUP. A complaint from the recipient of commercial e-mail, whether received directly, or through an anti-spamming organization, shall be evidence that the message was unsolicited. Cyxtera has no obligation to forward the complaint to the User, or to identify the complaining parties.

2.8 <u>Cyxtera Right of Action for Prohibited Actions</u>

The actions described in this Section II are non-exhaustive, and Cyxtera reserves the right to take appropriate action to remedy any conduct which it deems to be a violation of this AUP or otherwise may be harmful to the Services, its customers, or Internet users.

INDIRECT OR ATTEMPTED VIOLATIONS OF THE AUP, AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON BEHALF OF A USER, SHALL BE CONSIDERED VIOLATIONS OF THE AUP BY SUCH USER.

III. Cyxtera's Rights

3.1 <u>Suspension or Termination of Services</u>

If Users engage in conduct or a pattern of conduct, including without limitation repeated violations by a User whereby correction of individual violations does not, in Cyxtera's sole discretion, correct a pattern of the same or similar violations, while using the Services that, in Cyxtera's sole discretion, violates the AUP, or is otherwise illegal or improper, Cyxtera reserves the right to suspend and/or terminate the Services or the User's access to the Services. Cyxtera will generally attempt to notify the Customer of any activity in violation of the AUP and request that such Customer take whatever steps necessary to, or to get the User to, cease such activity; however, in cases where the operation of the Services is threatened or cases involving unsolicited commercial e-mail/spam, a pattern of violations, mail relaying, alteration of the User's source IP address information, denial of service attacks, illegal activities, suspected fraud in connection with the use of Services, harassment or copyright infringement, the Company reserves the right to suspend or terminate the Services or the User's access to the Services without notification.

In the event that Company becomes aware that any such material may violate the terms of this AUP and/or expose Company to civil or criminal liability including, without limitation, under the Digital Millennium Copyright Act ("DMCA"), Company reserves the right to block access to such material and suspend or terminate the access of any User creating, storing, copying, or communicating such material, including any User whom Company becomes aware the User has engaged in any of the foregoing activities multiple times.

Cyxtera reserves the right to avail itself of the safe harbor provisions of the DMCA. Cyxtera does not make any promise, nor does Cyxtera have any obligation, to monitor or police activity occurring using the Services and will have no liability to any party, including a User, for any violation of the AUP.

3.2 Investigation and Enforcement

Cyxtera has the right, but is not obligated, to strictly enforce this AUP through self-help, active investigation, litigation and prosecution. Company shall not be obligated to monitor or exercise any editorial control over any material stored, copied, or communicated using the Services, but reserves the right to do so. In addition, Cyxtera may take any other appropriate action against the User for violations of the AUP, including repeated violations wherein correction of individual violations does not, in Cyxtera's sole discretion, correct a pattern of the same or similar violations.

Company further reserves the right to conduct investigations into fraud, violations of the terms of this AUP or other laws or regulations, and to cooperate with legal authorities and third parties in the investigation of illegal or inappropriate activity using the Services, including disclosing the identity of the User that Company deems responsible for the wrongdoing.

3.3 Cooperation with Law Enforcement

Cyxtera may also access and disclose any information (including transactional information) related to a User's access and use of the Services if required by applicable law.

Cyxtera will cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal or inappropriate activity. Cyxtera reserves the right to disclose User information to the extent required by federal or state law. By using and accepting the Services, Customer consents to Company's disclosure to any law enforcement agency, of Customer's identity as the service provider of record (including basic contact information), as applicable, for any User about whom Cyxtera is required by applicable law to provide such information to such law enforcement agency. In instances involving child pornography, Cyxtera will comply with all applicable federal and state laws, including providing notice to the National Center for the Missing and Exploited Children or other designated agencies.

3.4 Filters and Service Information

Cyxtera reserves the right to install and use, or to have Customer install and use, any appropriate devices to prevent violations of this AUP, including devices designed to filter or terminate access to the Services. By accepting and using the Services and allowing Users to use the Services, Customer consents (on its own behalf and on behalf of all other Users) to allowing Company to collect service information and routing information in the normal course of its business, and to use such information for general business purposes.

3.5 Indemnification

The Customer agrees to indemnify, defend and hold harmless Company, its officers, directors, employees, agents, shareholders, licensors, and suppliers from and against all claims, liabilities, losses, expenses, damages and costs, including reasonable attorneys' fees, that arise from or are related to: (1) any violation by the Customer of this AUP or the acceptable use policy of any third party network provider contracted by Cyxtera in support of the Services; (2) any violation of any rights of a third party by the Customer; (3) any violation of applicable law; or (4) information or content that a Customer submits, posts, transmits or makes available through the Services. Notwithstanding anything in the Agreement to the contrary, Customer's obligations under this Section 3.5 shall not be subject to any limitations on liability under the Agreement, including, but not limited to, any liability cap or consequential, indirect, special or punitive damages waiver.

IV. Customer and User Responsibilities

4.1 Notice of Security Issues

Users are entirely responsible for maintaining the confidentiality of password and account information, as well as the security of their network. Users agree to immediately notify Cyxtera of any unauthorized use of their accounts or any other breach of security known to such User. If the User becomes aware of any violation of this AUP by any person, the User is required to notify Company.

4.2 Configuration

All Users of the Services are responsible for configuring their own systems to provide the maximum possible accountability. Cyxtera shall not be liable for any damage caused by such system configurations regardless of whether such configurations have been authorized or requested by Cyxtera. For example, Users should ensure there are clear "path" lines in news headers so that the originator of a post may be identified. Users should also configure their Mail Transport Agents (MTA) to authenticate (by look-up on the name or similar procedures) any system that connects to perform a mail exchange, and should generally present header data as clearly as possible. As another example, Users should maintain logs of dynamically assigned IP addresses. Users of the Services are responsible for educating themselves and configuring their systems with an effective level of security. Should systems at a User's site be violated, the User is responsible for reporting the violation and then fixing the exploited system. For instance, should a site be abused to distribute unlicensed software due to a poorly configured FTP (File Transfer Protocol) Service, the User is responsible for reconfiguring the system to stop the abuse.

4.3 Impending Security Event Notification

All Users of the Services are responsible for notifying Cyxtera immediately if they become aware of an impending event that may negatively affect the Services. This includes extortion threats that involve threat of "denial of service" attacks, unauthorized access, or other security events.

4.4 Complaints

In most cases, Cyxtera will notify its customer(s) of complaints received by it regarding an alleged violation of this AUP. You agree to, and to cause the applicable User to, promptly investigate all such complaints and take all necessary actions to remedy any violations of this AUP. Company may inform the complainant that you and/or the applicable User are investigating the complaint and may provide the complainant with the necessary information to contact you and/or the applicable User directly to resolve the complaint. Users are required to identify a representative for the purposes of receiving such communications.

V. Privacy

Because the Internet is an inherently open and insecure means of communication, any data or information a User transmits over the Internet may be susceptible to interception and alteration. Subject to Cyxtera's online Privacy Policy, we make no guarantee regarding, and assume no liability for, the security and integrity of any data or information a User transmits via the Service or over the Internet, including any data or information transmitted via any server designated as "secure".

VI. Miscellaneous Provisions

6.1 No Waiver and Severability of AUP

Failure by Cyxtera to insist upon or enforce strict performance of any provision of this AUP will not be construed as a waiver of any provision or right. Neither the course of conduct between the parties nor trade practice will act to modify any provision of this AUP. If any provision of this AUP is found to be unenforceable or invalid, this AUP's unaffected provisions will remain in effect.

6.2 Complaints and Contact Information

Any complaints regarding prohibited use or other abuse of the Services, including violation of the AUP, should be sent to Cyxtera at CustomerCare@Cyxtera.com or call Cyxtera at 800-884-3082. Please include all applicable information that will assist Cyxtera in investigating the complaint, including all applicable headers of forwarded messages. Sites experiencing live attacks from Cyxtera customers should call 800-884-3082 to submit a complaint as quickly as possible. Please state the urgency of the situation should you need immediate attention.

If you are unsure whether any contemplated use or action is permitted, please submit questions or comments to Cyxtera at CustomerCare@Cyxtera.com or 800-884-3082.