



**MASTER SERVICE AGREEMENT
ACCEPTABLE USE POLICY (AUP)**

ACCEPTABLE USE POLICY (AUP):

This Acceptable Use Policy (AUP) is incorporated by reference in your Master Service Agreement with CyberOne Data, LLC. **At its sole discretion, CyberOne Data, LLC may suspend or terminate this Agreement, with or without notice, if Client violates any terms or conditions of CyberOne Data, LLC's Service Level Agreement (SLA) and/or Terms of Service (TOS). If so terminated, no refunds will be made for pre-paid services.**

1. Overview: Our goal is to deliver enterprise quality services to all of our Clients. CyberOne Data, LLC is dedicated to protecting the source and distribution of information and protecting the rights and privileges of those utilizing the Internet including the storage, distribution and exchange of information (content). CyberOne Data, LLC has no intent to act as the content police; our duty in the process of information dissemination is simply to act as a conduit between interested parties. Notwithstanding anything found herein, CyberOne Data, LLC strives to follow all local, state and federal laws pursuant to the services delivered over the Internet and directly related to our network and internal systems. The purpose of this AUP is to inform all Clients of acceptable, anticipated Client usage. Due to the countless possibilities of maintaining a network comprised of hundreds or thousands of servers, this AUP is intended to act as a guideline to service and shall be not deemed all encompassing.

2. Emailing, Texting, IM and SPAM: Unsolicited commercial advertisements (spam) are not allowed in communications and can result in account termination at CyberOne Data, LLCs sole discretion. CyberOne Data, LLC takes a zero-tolerance approach to spam originating from our servers or for spam advertising of domains hosted on our servers. The following activities are not allowed:

a. Unsolicited bulk or commercial messages ("spam"). This includes, but is not limited to, bulk mailing of commercial advertising, informational announcements, charity requests, petitions for signatures, and political or religious tracts. Such messages may only be sent to those who have explicitly requested it from your domain.

b. Forging, altering or removing electronic mail headers is prohibited. Any domain sending stealth spam may be immediately terminated without warning and without refund.

c. Sending numerous copies of the same or substantially similar message with the intent to disrupt a server or account ("mail bombing").

d. Spamming Newsgroups: Commercial advertisements are unwelcome in most Usenet discussion groups and on most email mailing lists. Inappropriate posting may result in account cancellation. See the newsgroup or mailing lists charter for whether advertising is allowed or prohibited. "Spamming," or sending a message to many different off-topic newsgroups, is particularly unethical and will be treated as such.

e. Communications may not be used to harass or intimidate others. Harassment, whether through language, frequency of messages, or size of messages, is prohibited. Sending a single unwelcome message may be considered harassment. If a recipient asks to stop receiving email, you must not send that person any further messages.

f. Providing spamware (software used to send bulk email or software used to harvest email addresses) or links to sites providing spamware is strictly prohibited and subject to demand for removal or account termination.

g. CyberOne Data, LLC will handle all complaint resolution with upstream bandwidth providers and anti-spam organizations related to Client's use of CyberOne Data, LLCs IP's and Bandwidth. CyberOne Data, LLC shall provide Client with an email notification of any complaints received, and Client shall (a) provide CyberOne Data, LLC, with all opt-in information related to such complaint within twenty-four (24) hours; and (b) permanently remove any associated end-user email addresses from all of Client's opt-in email lists. Client shall not add a Removed Address back onto its Lists or attempt to deliver any email to a Removed Address even if Client receives a future opt-in request from such Removed Address. CyberOne Data LLC will not under any circumstances provide Client's information to any upstream bandwidth providers, anti-spam organizations, or to ARIN for SWIP purposes unless specifically requested by Client.

h. If a Spamhaus (<http://spamhaus.org/sbl>) SBL or UCE Protect (<http://www.uceprotect.net>) Network Level 2 or 3 listing occurs and removal of Client from IP Space is required by upstream provider, CyberOne Data, LLC will immediately null-route all affected IP space. There will be no refunds for services and Client is responsible for paying entire contract in full. In the case of a null route or SBL / UCE-Protect listing or any other client-activity based cause resulting in the loss of the IP space, Client agrees to forfeit the current month's service payment due to Client violation of the Acceptable Use Policy. Client may, at CyberOne Data, LLCs sole discretion, procure new IP space and service(s) under a new Service Order Form.

Note: If the services of another provider are used (including but not limited to the use of address lists obtained from a third party vendor or provider) to promote a website hosted by or through CyberOne Data, LLC (spamvertising), then the provisions of the above Policy shall apply as if the spam were sent through our servers.

Damages:

All AUP Violations: CyberOne Data, LLC reserves the right to charge \$50 for the 1st incident. Subsequent/repeat offenses will incur increased violation fees in \$25 increments.

Spam Violations: CyberOne Data, LLC reserves the right to charge \$1 to \$100 per spam message sent in addition to the AUP Violation.

3. Direct AUP Violations: The following list represents direct violations of this AUP:

a. Email Bombing: The sending, return, bouncing or forwarding of email to specified user(s) in an attempt to interfere with or over flow email services.

b. Illegal Use: Any use of services in a manner which is defined or deemed to be statutorily illegal. This includes, but is not limited to: death threats, terroristic threats, threats of harm to another individual, multi-level marketing schemes, "ponzi schemes", invasion of privacy, credit card fraud, racketeering, defamation, slander, and other illegal activities.

c. Child Pornography: CyberOne Data, LLC has a zero-tolerance policy on child pornography and related sites. The hosting of child pornography or related sites or contact information is in direct violation of federal law.

d. Threats & Harassment: The CyberOne Data, LLC network can be utilized for any type of individual, organizational or business use. This does not include threats to or harassment of individuals, organizations or businesses, unless it falls within the bounds of protected free speech under the First Amendment. CyberOne Data, LLC seeks to serve only as the medium of exchange for information and refrains from decisions on freedom of speech.

e. Fraudulent Activities: CyberOne Data, LLC prohibits utilizing services for fraudulent activities.

f. Denial of Service: CyberOne Data LLC prohibits the use of services for the origination or control of denial of service attacks or distributed denial of service attacks.

g. Terrorist Websites: CyberOne Data LLC prohibits the use of services for the hosting of terrorist-related web sites. This includes sites advocating human violence and hate crimes based upon religion, ethnicity, or country of origin.

h. Distribution of Malware: CyberOne Data LLC prohibits the storage, distribution, fabrication, or use of malware including virus software, root kits, password crackers, adware, key stroke capture programs and other programs normally used in malicious activity. Programs used in the normal ordinary course of business are deemed acceptable.

i. Phishing: CyberOne Data, LLC prohibits any activity associated with phishing or systems designed to collect personal information (name, account numbers, usernames, passwords, etc.) under false pretense. Splash pages, phishing forms, email distribution, proxy email or any relation to phishing activities will result in immediate removal.

j. HYIP or Ponzi Schemes: High Yield Investment Plans or Ponzi schemes with the intent to defraud end users are illegal and not allowed on the network. This includes hosting, linking and/or advertising via email websites or schemes designed to defraud.



k. TOR, I2P, other Anonymization Services: While CyberOne Data, LLC does understand that anonymization services provide vital access necessary for people worldwide, the untraceable nature can often make these services sources of abuse. As there is no way to mitigate or restrict the traffic originating from these services, abuse issues may incur fees if not resolved by the client upon notification.

4. Abuse of Bandwidth Allotments: CyberOne Data, LLCs Clients are privileged to be offered large amounts of bandwidth and monthly transfers to their servers. The intention of CyberOne Data, LLC is to provide large redundant bandwidth allotments to businesses and consumers to serve as connections for their websites and web documents. You, the Client, are responsible for any unauthorized access to your account resulting in bandwidth overages, storage and/or email usage exceeding the limits outlined in your Service Order Form and resultant charges. The Client will be billed at \$20/Mbps for any overage incurred.

5. Public Network: The primary purpose of the CyberOne Data, LLC Public Network is to transmit information to and from Client servers and data storage services. Proper use of the Public Network is to utilize the network in any way so long as Client does not violate any local, state, or federal laws or generate harm to the network or interfere with the use of services of other users utilizing the same network. All Clients are granted equal access to the Public Network. Violation, misuse, or interference of the Public Network shall be considered a violation of the AUP.

6. Security Services: The primary purpose of the CyberOne Data, LLC security services is to assist the Client in the protection, management, update, and overall stability of their environment. CyberOne Data, LLC supplies various patches and updates to the infrastructure and CyberOne Data, LLC managed equipment. Many security services are offered for a fee and are covered via the terms of the individual services. These services include, but are not limited to: firewalls, host intrusion detection services, service monitors and other similar type products and services. Outside of the global network security services described above, Clients are required and obligated to maintain security related to Client managed servers. The management of dedicated servers requires basic security management including password management, port management, OS updates, application updates, security policy settings and more. The Client is ultimately responsible for individual server security unless contracted security services are purchased. Any violation of the security services included in basic services shall be considered a violation of the AUP.

7. Server Content: CyberOne Data, LLC does not actively monitor dedicated server content for review. CyberOne Data, LLC believes in the free dissemination of information via our services. Dedicated server content will only be reviewed upon complaint by verified third parties. Content that does not violate local, state and federal law or the AUP is deemed in compliance and shall remain intact. Legal adult content is allowed on CyberOne Data, LLC dedicated servers. Content deemed in violation shall be considered a violation of the AUP.

8. DNS Services: CyberOne Data, LLC may supply name services for Clients purchasing dedicated services. These name services usually include the use of authoritative name servers for public resolution of domain names and private domain name resolvers located on our network. The DNS services are fully managed and maintained by CyberOne Data, LLC with Client specific domain name management through the online Client portal. In rare instances, where extreme intensive loads (DNS lookups) utilize disproportionate resources of the redundant DNS systems, CyberOne Data, LLC will notify Client of potential violation of this AUP. Clients requiring such DNS services will be instructed to perform dedicated DNS services on Client managed equipment. Violation of DNS services shall be considered a violation of the AUP.

9. IP Addresses: All Internet Protocol (IP) Addresses are owned or leased and managed by CyberOne Data, LLC, Inc. IP Addresses are non-transferable from CyberOne Data, LLC, and Client retains no ownership or transfer rights to IP Addresses. Attempted use of IP addresses not originally allocated for use or IP addresses used on non-assigned VLANs or servers is a violation of this AUP.



10. Unauthorized Access: Use of the CyberOne Data, LLCs services to access, or to attempt to access the accounts of others, or to penetrate, or attempt to penetrate security measures of CyberOne Data, LLC or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data, is expressly prohibited and the offending account is subject to immediate termination. The outstanding balance of any contracts/account will immediately become due. DMCA: CyberOne Data, LLC takes the protection of copyright seriously. Under the DMCA, we have an obligation to respond to any claims of infringement that comply with the form prescribed by law, and to remove access to any infringing content that is not disputed with a valid counter claim. If you have a DMCA complaint you would like to file with us, please follow the guidelines available here: <https://www.law.cornell.edu/uscode/text/17/512#c.3>.

11. Reporting Violation of the Acceptable Use Policy: CyberOne Data, LLC accepts reports of alleged violations of this AUP via email sent to abuse@cyberonedata.com. Reports of alleged violations must be verified and must include the name and contact information of the complaining party, and the IP address or website allegedly in violation, and description of the violation. CyberOne Data, LLC owes no duty to third parties reporting alleged violations due to lack of privacy in contract law. CyberOne Data, LLC will review all verified third party reports and will take appropriate actions.