ACCEPTABLE USE POLICY (AUP)

PREAMBLE

A. This AUP is included as part of, and shall be read together with, the Terms and Conditions.
B. As such, any capitalised terms used herein shall bear the meanings ascribed there to in the terms and conditions of use, unless otherwise defined herein.

1. AGREEMENT TO THIS AUP

1.1. You agree that you will only use our services in a manner consistent with this AUP and that your failure to do so may be grounds for us to suspend or discontinue service provision.

1.2. This AUP is intended to help enhance the use of the Internet by preventing unacceptable use. It is not a "terms of service" or a billing guideline. Please refer to your Terms of Service for terms and conditions applicable to your Internet Service.

1.3. PLEASE READ THIS AUP CAREFULLY BEFORE ACCESSING THE SERVICE. BY ACCESSING THE SERVICE, YOU AGREE TO BE BOUND BY THIS AUP. IF YOU DO NOT WISH TO BE BOUND BY THIS AUP, YOU MAY NOT ACCESS OR USE THE SERVICE.

1.4. This AUP applies to Internet Services ("**Services**") provided by CoCre8 Technology Solutions ("**Service Provider**"). Your use of the Services indicates your acceptance of and agreement to abide by this AUP. It is designed to help protect the Service, Service Provider customers and the Internet community from irresponsible or illegal activities. The Service Provider may modify this AUP from time to time. In the event of any inconsistency between this AUP and the terms of any service agreement, this AUP shall govern and control to the extent of the inconsistency.

2. GENERAL POLICY

The Service Provider reserves the right in its sole discretion to deny or restrict your use of the Services, or to immediately suspend or terminate your Services, if the use of your Services by you or anyone using it, in our sole discretion violates your Terms of Service or other Service Provider policies, is objectionable or unlawful, interferes with the functioning or use of the internet or Service Provider network by Service Provider or other users or violates the terms of this AUP.

3. ILLEGAL AND PROHIBITED USE

3.1. This section is used to address actions, content and or practices that are prohibited by law and by rules set forth by the Service Provider. Please review the sections below before using the Service Provider's Services or networks. The restrictions are not negotiable. Not all Services provided by the Service Provider are listed or mentioned, but are bound by this document.

3.2. Users found to engage in activities that the Service Provider determines, in its sole discretion, are in violation of this AUP will have their accounts terminated. Violators may also be subject to any appropriate legal action and/or consequences. The Service Provider reserves the right to co-operate with legal authorities and/or injured third parties in the investigation of any suspected illegal activity or civil wrong doing. Activities or use of Services considered by the Service Provider to be a violation of this AUP are as follows, but are not limited to:

3.2.1. to post or transmit information or communications that, whether explicitly stated, implied, or suggested through use of symbols, are obscene, indecent, pornographic, sadistic, cruel, or racist in content, or of a sexually explicit or graphic nature; or which espouses, promotes or incites bigotry, hatred, terrorism or racism; or which might be legally actionable for any reason;

3.2.2. to post, transmit, download or view any material whatsoever pornographic in nature involving actual images of children or minors or digitally or otherwise artificially created or manipulated images of children or minors, or any material whatsoever that may be deemed obscene under applicable law;

3.2.3. to access or attempt to access the accounts of others, to spoof or attempt to spoof the URL or DNS or IP addresses of Service Provider or any other entity, or to attempt to

penetrate or penetrate security measures of Service Provider or other entities' systems ("hacking") whether or not the intrusion results in corruption or loss of data;

3.2.4. to introduce viruses, worms, harmful code and/or Trojan horses on the Internet;

3.2.5. to violate Service Provider or any third party's copyright, trademark, proprietary or other intellectual property rights, including trade secret rights;

3.2.6. to use any name or mark of Service Provider, its parent, affiliates or subsidiaries, as a hypertext link to any Web site or in any advertising publicity or other commercial manner;

3.2.7. to use the Service or the Internet in a manner intended to threaten, harass, intimidate or terrorize;

3.2.8. to make false or unverified complaints against any Service Provider subscriber, or otherwise abusing any of the Service Provider complaint response procedures;

3.2.9. indirect or attempted violations of this AUP;

3.2.10. reselling of services provided by the Service Provider;

3.2.11. Services used to transmit, retransmit, distribute, post, or store any material that in the judgment of the Service Provider is threatening, libelous, defamatory, or otherwise objectionable including but not limited to child pornography and advocating unlawful activity against any persons, animals, governments or businesses;

3.2.12. harassment of users, employees, or of others will not be tolerated;

3.2.13. actions and/or Services prohibited by federal, state and local law;

3.2.14. distribution, posting, copying or dissemination of copyrighted material, including, but not limited to, movies and/or music;

3.2.15. inhibiting any other person's use of the Service provided by the Service Provider is prohibited;

3.2.16. participation in illegal gambling, lottery or other similar activities;

3.2.17. transmission of scams such as "Make Money Fast" schemes;

3.2.18. making fraudulent offers; and/or

3.2.19. the attempt to access the accounts of other or other computers and/or networks to penetrate security measures, whether or not the intrusion results in damage.

3.3. The Service Provider reserves the right to limit, restrict and/or prohibit Services it provides to customers, as the Service Provider determines necessary. The restrictions mentioned apply to all users unless specifically documented.

4. EMAIL

4.1. The Service Provider reserves the right to limit the file size of individual email mailboxes at its sole discretion. Individual email mailboxes found over the limit will be subject to deletion without notice. Deleted email will not be restored or saved.

4.2. The Service Provider reserves the right to limit the maximum transfer limit of any one message in its sole discretion.

4.3. The Service Provider reserves the right to reject or filter email based on source address and content.

4.4. Examples include, but are not limited to, virus filtering and blocking open relay mail servers.

4.5. The Service Provider will not provide back-ups of a customer's email.

4.6. Email usage will be limited to 300 messages sent out per user, per day.

4.7. The email webclient (https://mail.domain.x) is the only email client supported by the Service Provider. Third party email client use is unsupported by the Service Provider. Use of third party email clients is strictly at the users own risk.

4.8. The Services may not be used to transmit, retransmit, or distribute by e-mail or any other method any material that violates any condition of this AUP in the sole judgment of ISP. Activities considered by Service Provider to be a violation of this AUP are as follows, but are not limited to:

4.8.1. any unsolicited e-mail, whether commercial or otherwise, including, but not limited to, bulk mailing of commercial advertising, informational announcements, and political tracts.

4.8.2. Solicited e-mail that contains material that otherwise violates this AUP or any e-mail that falsifies the address or other information; harassing e-mail, whether through language, frequency, or size of messages;
4.8.3. any e-mail “chain letters” or other “pyramid schemes”;
4.8.4. e-mail relayed without the express permission of that site, service, system or network;
4.8.5. e-mailing the same or similar messages to one or more newsgroups (also known as “cross-posting” or “multiple posting”);
4.8.6. e-mail containing false or misleading statements, claims, or representations; and/or
4.8.7. forging header information including, but not limited to, any attempt to circumvent the approval process for posting to a moderated newsgroup.

5. **SPAM**

5.1. Service Provider has a “zero tolerance” policy for SPAM. Any User of the Service Provider’s Services found to be actively distributing or engaged in the mass distribution of unsolicited emails without consent of the intended receiver may have their account(s) terminated and all future access to Service Provider’s Services and network revoked. You may not use the Service or any Equipment or Software provided by Service Provider:
5.1.1. to send e-mail of a personal, bulk or commercial nature, including, without limitation, bulk mailings of commercial advertising, informational announcements, charity requests, political or religious messages, and petitions for signatures, except to those who have requested such e-mails via a confirmed opt-in subscription process maintained by You;.
5.1.2. to send e-mail or other messages to someone who has indicated that he or she does not want to receive messages from You;
5.1.3. to collect or receive responses from unsolicited e-mail messages (even if such e-mail was sent from accounts on other Internet service providers or e-mail Services) that violate the Agreement or this AUP or the terms of use under the other Internet service provider or e-mail service from which it was sent;
5.1.4. to conduct “mail bombings” (e.g., to send more than ten copies of the same or substantially similar message, or to send very large messages or files, with the intent of disrupting a server or account);
5.1.5. to send or forward make-money-fast schemes or chain/pyramid letters (whether or not the recipient requests it);
5.1.6. to harvest e-mail addresses or personal information of other Service Provider subscribers or the subscribers of any other network;
5.1.7. to use another Internet site’s mail server to relay mail without the express permission of the owner of that Internet site; and/or
5.1.8. to use e-mail or the internet in violation of federal law or the rules of the Federal Communications Commission.
5.2. Multiple logons are restricted. Users are only allowed to logon once with the same account. Accounts establishing concurrent connections will be disconnected. Abuses of this service may be subject to account termination.

6. **BROADBAND**

6.1. The Service Provider restrictions to Broadband Services are:
6.1.1. multiple logons are restricted;
6.1.2. users are only allowed to logon once with the same account; and/or
6.1.3. accounts establishing concurrent connections will be disconnected.
6.2. Abuses of this service may be subject to account termination.
6.3. Modifications of the CPE / Broadband Router / modem in ways other than advised by the manufacturer are restricted.

7. **SERVING**

7.1. Serving of any kind is NOT allowed without express written consent from the Service Provider. Consent should be given in a separate service contract and should be producible by the customer upon request from the Service Provider.

7.2. Serving constitutes:

7.2.1. email servers;

7.2.2. web – HTTP servers;

7.2.3. domains;

7.2.4. certificates;

7.2.5. backups; and/or

7.2.6. other Listening IP Services.

8. UNAUTHORIZED SHARING

You agree not to allow others to use any of the Services provided including, but not limited to, sharing your account user name and password or broadband access via any type of networking device (router, gateway, wireless access point, etc.). You may at your own risk and responsibility permit other members of your household to access the Services and utilize some networking devices approved by the provider for use within your household only. You as the account holder shall ensure that other such users are aware of and comply with these terms of use, and you agree to be held responsible for any activity or use of the Services on that account, whether or not authorized by you.

9. COMMERCIAL USE

9.1. Re-selling the Service Provider's Services or offering use of the Service Provider's Services for adding value to a commercial entity without the Service Provider's authorization is prohibited. The Service Provider's Services are designed for the account holder's use of the Internet and may not be used for commercial purposes without the Service Provider's explicit consent.

9.2. You also agree not to use the Service Provider's Services for operation as an Internet Service Provider (ISP), or for any other business enterprise including, without limitation, IP address translation or similar facilities intended to provide access, operating or allowing others to operate servers of any type, or any other device, equipment and/or software providing server-like functionality in connection with the Service Provider's Services, unless expressly authorized.

10. **OTHER**

Other Services not specifically listed in this AUP but that are provided by the Service Provider are bound by this AUP.

11. COMPLIANCE WITH THE AUP OF UPSTREAM PROVIDERS

The AUP of the Service Provider's upstream providers also bind the Service Provider's users. An "upstream provider" is any company that provides the Service Provider bandwidth and/or other services.

12. SYSTEM AND NETWORK SECURITY

Violations of system or network security are prohibited and may result in criminal and civil liability. Service Provider will investigate incidents involving such violations and may involve and will co-operate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

12.1. port scanning, probes, data capture, denial of service, access of restricted systems.

12.2. attempted access of systems not previously given access to;

12.3. anything deemed "hacking" or "cracking" to the systems, network or users;

12.4. unauthorized access to or use of data, including any attempt to circumvent user authentication or security of any host, network, or account (hacking, cracking, port scans, or flood pings);
12.5. unauthorized monitoring of data or traffic;
12.6. interfering with service to any user, host, system or network;
12.7. conducting denial of service attacks;
12.8. any attempt to disrupt service including, but not limited to, distributing or introducing viruses, worms, or other harmful software; and/or
12.9. access by using artificial means, involving software, programming, or any other method.

13. USER RESPONSIBILITY

13.1. Users need to be aware that they do not operate in a vacuum. Safe practices need to be taken by the users to protect themselves and others.
13.2. Users are responsible for account passwords and should keep them safe.
13.3. Do NOT share account information.
13.4. Do NOT leave username and passwords in the open. If a user feels that the account was compromised, the username and or password should be changed at once.
13.5. Do NOT "save" user names or passwords. Each should be entered at each login.
13.6. Users are responsible for protecting their own equipment. Anti-virus software and personal firewalls are not required but strongly encouraged.
13.7. Users are responsible for any misuse of Service Provider Services that occurs through user's account.
13.8. Users are responsible for protecting their accounts and must take steps to insure that others do not gain unauthorized access to user's account or misuse Service Provider's Services.

14. ADMINISTRATIVE DISCRETION

The Service Provider administrators, staff, and executives have sole and final discretion over all aspects of service, the network, and this AUP. The Service Provider reserves the right to terminate any account or service without cause or prior notice.

15. VIOLATIONS AND MONITORING

15.1. The Service Provider does not intend to actively monitor the content of web sites, e-mail, news groups, or material created or accessible over its Services. The Service Provider reserves the right to monitor such Services or any Services on or within our network.

15.2. Reporting Violations and complaints:
Violations, attempted violations, and/or concerns should be addressed to abuse@cocre8.com via Email.

15.3. When reporting anything to Service Provider please include:
15.3.1. the internet protocol address used to commit the alleged violation; and
15.3.2. the date, time and time zone of such violation.
15.4. Evidence of the violation, including, if applicable, full headers from emails, firewall logs, traffic dumps (example, the *.enc files generated by Network Ice's Black Ice program or "hex" dump from any other firewall or IDS system) or information pertaining to the events in question.
15.5. Do not send excerpted parts of a message; sending the entire message with full headers helps prevent misunderstandings based on incomplete information or information taken out of context.
15.6. The Service Provider has sole judgment and discretion on how we enforce this AUP. Guidelines as to punishment and legal action will be within the Service Provider's legal department and administrative department discretion.