Acceptable Use Policy ("AUP")

GENERAL

This document is the property of Cynaptic Ltd and is an acceptable use policy ("AUP") setting out the terms between you and us under which you may access our service(s) (the "Services"). You can use the contents of this document only for the purpose of governing your use of our Services. This AUP applies to all our clients and users of our services. You are responsible for violations of this AUP by your or anyone using your system, whether authorised by you or not. If you have any questions, please contact us at legal@cynaptic.eu

Your use of our services means that you accept, and agree to abide by, all the policies in this AUP.

Our services are operated and provided by Cynaptic (we or us). We are registered in Cyprus under company number HE326005 and we have our registered office at: Kinyras 19, Kyprianou House, 8011, Paphos, Cyprus. Our main trading address is, 33 Nikolaou Nikolaidi Ave., Office 9, 8010 Paphos, Cyprus. Our Address for official correspondence is PO Box 61085, Kato Paphos, 8310, Paphos, Cyprus. Our VAT number is: CY 10326005E.

1.INTERNET ABUSE

You may use our Services only for lawful purposes. You may not use our network to engage in illegal, abusive, or irresponsible behaviour, including:-

1.1. unauthorised access to or use of data, services, 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 authorisation of the owner of the system or network;

1.2. monitoring data or traffic of any network or system without the authorisation of the owner of the system or network;

1.3. interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

1.4. use of an internet account or computer without the owner's authorisation;

1.5. collecting information by deceit, including, but not limited to internet scamming (tricking other people into releasing their passwords), password robbery, phishing, securing hole scanning and port scanning;

1.6. use of any false, misleading or deceptive TCP-IP packet header or any part of the heading information in an e-mail or newsgroup posting;

1.7. use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;

1.8. any activity or conduct that is likely to result in retaliation against our network;

1.9. any activity or conduct that is likely to be or is in breach of any applicable national (CY) or international laws, codes or regulations including data protection;

1.10. introducing intentionally or knowingly into our or any system any virus or other contaminating program such as but not limited to (Trojan horses, worms, time-bombs, keystroke loggers, spyware) or fail to us an up to date virus-scanning program on all material downloaded from the Services;

1.11. is used to send unsolicited e-mails ("Spam");

1.12. misrepresenting yourself as other computer networks and/or users; or

1.13. any activity or conduct that unreasonably interferes with our customers' use of our Services.

2. SECURITY

2.1. You must take reasonable security precautions.

2.2. Passwords should consist of at least eight (8) mixed alpha and numeric characters with case variations. You should not permit a common word to be used as a password. You must protect the confidentiality of your password and you should change your password regularly.

3. BULK COMMERCIAL E-MAIL

3.1. Under the European Directive 2002/58/CE of 12 July 2002 (the "Directive") on privacy and electronic communications, the use of e-mail for direct marketing is only allowed to recipients who have given their prior consent. We acknowledge that market research is not considered as direct marketing within the meaning of the Directive above and therefore, the requirements set out below do not apply to bulk e-mails for market research purposes. You must obtain our advance approval in writing for any bulk commercial e-mail other than for market research purposes, for which you must be able to demonstrate the following to our reasonable satisfaction:-

3.1.1. your intended recipients have given their consent to receive e-mail via some affirmative means, such as an opt-in procedure;

3.1.2. your procedures for soliciting consent include reasonable means to ensure that the person giving consent is the owner of the e-mail address for which the consent is given;

3.1.3. you retain evidence of the recipient's consent in a form that may be promptly produced within 72 hours of receipt of recipient's or our request(s) to produce such evidence;

3.1.4. the body of the e-mail must include information about where the e-mail address was obtained, for example, "You opted in to receive this e-mail promotion from our Website or from one of our partners sites", and information on how to request evidence of the consent, for example "If you would like to learn more about how we received your e-mail address please contact abuse@yourdomain.com";

3.1.5. you have procedures in place that allow a recipient to revoke their consent – such as a link in the body of the e-mail, or instructions to reply with the word "Remove"

in the subject line and such revocations of consent are implemented within 72 hours;

3.1.6. you must post an abuse@yourdomain.com e-mail address on the first page of any Website associated with the e-mail, you must register that address at abuse.net and you must promptly respond to messages sent to that address;

3.1.7. you must have a Privacy Policy posted for each domain associated with the mailing;

3.1.8. you must have the means to track anonymous complaints;

3.1.9. you may not obscure the source of your e-mail in any manner. Your e-mail must include the recipient's e-mail address in the body of the message or in the "TO" line of the e-mail.

3.2. These policies apply to messages sent using our Services or network, or to messages sent from any network by you or any person on your behalf that directly or indirectly refer the recipient to a site hosted via our Services.

3.3. You may not use third party e-mail services that do not have similar procedures for all its customers.

3.4. We may test and monitor your compliance with these requirements, including requesting opt-in information from a random sample of your e-mail list at any time.

4. UNSOLICITED E-MAIL

4.1. You may not send any unsolicited e-mail, whether commercial or non-commercial in nature, to any person who has indicated that they do not wish to receive it.

5. VULNERABILITY TESTING

5.1. You may not attempt to probe, scan, penetrate or test the vulnerability of our system or network (or anyone else's) or to breach security or authentication measures whether by passive or intrusive techniques without our prior written consent.

6. N/A

7. CONTENT

7.1 Cynaptic does not actively monitor server content for review. Cynaptic believes in the free dissemination of information via our services. Content will only be reviewed upon complaint by verified third parties.

7.2 Content that does not violate UK law or this AUP is deemed in compliance and shall remain intact.

7.3 Adult content is allowed on Cynaptic services, as long as Content is not contrary to EU law, statute, or regulation. Content deemed in violation will be addressed pursuant to the Methods of Resolution under this AUP as set forth below in Table A

7.4 The following list represents per se direct violations of this AUP and will be subject to immediate redress under one or more of the Methods of Resolution as described in this

AUP and as set forth below in Table A. Note: Cynaptic is not required to follow the Methods of Resolution for Hourly Services, and reserves the right to immediately terminate Hourly Services based on violations of this AUP.

7.4.1 Copyright and Trademark Infringement: Direct copyright infringement and trademark infringement are direct violations of Cynaptic's AUP.

7.4.2 Unsolicited Email: The sending or receiving of mass unsolicited email (SPAM) Is a direct violation of Cynaptic's AUP. This includes the direct sending and receiving of such messages, support of such messages via web page, splash page or other related sites, or the advertisement of such services as defined in sections 3 and 4 above.

7.4.3 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 is a direct violation of Cynaptic's AUP.

7.4.4 Proxy Email (SPAM): The use of dedicated services to proxy email unsolicited users is a direct violation of Cynaptic's AUP. Proxy email is defined as the use of dedicated services to act in concert with other services located inside and outside the network to achieve mass unsolicited email (SPAM) to unrelated third parties.

7.4.5 UseNet SPAM: The use of dedicated services to send, receive, forward, or post UseNet unsolicited email or posts is a direct violation of Cynaptic's AUP. This includes UseNet services located within the Cynaptic network or unrelated third party networks.

7.4.6 Illegal Use: Any use of dedicated services in a manner which is defined or deemed to be statutorily illegal is a direct violation of Cynaptic's AUP. 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, and other common illegal activities.

7.4.7 Child Pornography: Cynaptic 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 international law and Cynaptic's AUP.

7.4.8 Threats & Harassment: The Cynaptic 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. Cynaptic seeks to serve only as the medium of exchange for information and refrains from decisions on freedom of speech.

7.4.9 Fraudulent Activities: Cynaptic prohibits utilizing dedicated services or network services for fraudulent activities. Participation in fraudulent activities is in direct violation of international law and Cynaptic's AUP.

7.4.10 Denial of Service: Cynaptic absolutely prohibits the use of dedicated services or network services for the origination or control of denial of service attacks or distributed denial of service attacks. Any relation to DOS or DDOS type activity is a direct violation of Cynaptic's AUP.

7.4.11 Terrorist Websites: Cynaptic prohibits the use of dedicated 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.

7.4.12 Distribution of Malware: Cynaptic prohibits the storage, distribution, fabrication, or use of malware, including without limitation, 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. Example: Security Company hosting at Cynaptic analyzes the latest root kit for new security analysis/software.

7.4.13 Phishing: Cynaptic strictly 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.

7.5 Reporting Violation of the Acceptable Use Policy: Cynaptic accepts reports of alleged violations of this AUP via email sent to support@cynaptic.eu. 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. Unless otherwise required by law, Cynaptic owes no duty to third parties reporting alleged violations due to lack of privity in contract law. Cynaptic will review all verified third party reports and will take appropriate actions as described within Methods of Resolution as set forth in Table A below or within its sole discretion.

Table A: Methods of Resolution for Violations of Cynaptics' Acceptable Use Policy

Cynaptic understands the challenges of hosting companies, resellers, businesses, organizations and other customers who may have third party violations occur due to the nature of their business. The goal of our Methods of Resolution is to mitigate service interruptions while resolving potential violations under this AUP. Our sales, support and abuse staffs are dedicated to working with the Customer in resolving potential violations, and are available via phone, ticket, or email. The Methods of Resolution below form the framework for resolving all potential violations. Timing for resolution differs according to the degree of the violation, the nature of the violation, involvement of law enforcement, involvement of third party litigation, or other related factors. Overall, Cynaptic is dedicated to working with the Customer in resolving all potential violations prior to any service interruptions.

Step 1: First alleged violation of AUP: an email will be sent from Cynaptic to provide the Customer's master user with information regarding the potential violation of Cynaptic's AUP. This is often a fact-finding email requiring further information or notifying Customer of the potential violation and the required actions to resolve the issue.

Step 2: Acknowledgement of violation of AUP: a ticket is generated under the Customer's master user account with information specific to the violation. This ticket will also include any additional facts about the situation and will notify Customer of the action required to resolve the violation.

Step 3: Violation of AUP disregarded, not properly addressed, or continuing violation if a ticket has been disregarded, not properly addressed, or resolved by the Customer for a specified period of time: Cynaptic engineers will turn the public network port to the specified dedicated services off. Access to the dedicated services may then be achieved through the secure private service network for Customer resolution. As soon as the violation is addressed, the public access shall be restored and service will continue as normal.

Step 4: Failure to address violation and resolve violation: if Customer fails to address the violation AND fails to resolve the violation, a suspension of services shall occur. This is a last resort for Cynaptic and only results when the Customer completely fails to participate in Cynaptic's resolution process. A permanent suspension of services includes reclamation of all dedicated services and the destruction of Customer's data.

Disclaimer: Cynaptic retains the right, at its sole discretion, to refuse new service to any individual, group, or business. Cynaptic also retains the right to discontinue service to Customers with excessive and/or multiple repeated violations

8. EXPORT CONTROL

The Services may not be used by persons, organisation, companies or any such other legal entity or unincorporated body, including any affiliate or group company, which violates export control laws and/or is:-

8.1. located in Iran, Cuba, Sudan, Syria, North Korea (and/or any other country which at our discretion should be added if itself already subject to either EU and/or US sanctions of any kind); and/or

8.2. involved with or suspected of involvement in activities or causes relating to:-

8.2.1. illegal gambling;

8.2.2. terrorism;

8.2.3. narcotics trafficking;

8.2.4. arms trafficking or the proliferation of weapons of mass destruction; including any affiliation with others whatsoever who sponsor or support the above such activities or causes.

9. COPYRIGHT MATERIAL

9.1. You may not use our network or equipment to download, publish, distribute, or otherwise copy in any manner any text, music, software, art, image or other work protected by copyright law unless:-

9.1.1. you have been expressly authorised by the owner of the copyright for the work to copy the work in that manner; and

9.1.2. you are otherwise permitted by copyright law to copy the work in that manner.

9.2. We will suspend and/or terminate the Service of copyright infringers in accordance with the MHSA.

10. COOPERATION WITH INVESTIGATIONS AND LEGAL PROCEEDINGS

10.1. We may monitor any content or traffic belonging to you or to users for the purposes of ensuring that the Services are used lawfully. We may intercept or block any content or traffic belonging to you or to users where Services are being used unlawfully or not in accordance with this AUP and you do not stop or provide us with an acceptable reason within 7 days (including bank holidays and/or weekends) of receipt of a formal written notice from us.

10.2. We may without notice to you:-

10.2.1. report to the appropriate authorities any conduct by you that we believe violates any applicable law and/or regulation; and

10.2.2. provide any information we have about you, or your users or your traffic and cooperate in response to a formal or informal request from a law enforcement or regulatory agency investigating any such activity, or in response to a formal request in a civil/criminal action that on its face meets the requirements of such a request.

10.3. If we are legally required to permit any relevant authority to inspect your content or traffic, you agree we can do so, however, where possible without breaching any legal or regulatory requirement we may give you reasonable prior notice of such requirement and an opportunity to oppose and/or attempt to limit such inspection in each case to the extent reasonably practicable.

11. CONSEQUENCES OF VIOLATION OF AUP

11.1. You are strictly responsible for any and all use of your Services in breach of this AUP, including use by your customers and any unauthorised use that you could not have prevented (whether reasonable or not).

11.2. We will determine, in our discretion, whether there has been a breach of this AUP through your use of our Services. When a breach of this AUP has occurred, we may take such action as we deem appropriate.

11.3. Failure to comply with this AUP constitutes a material breach of the terms of upon which you are permitted to use our Services and may result in our taking all or any of the following actions:-

11.3.1. immediate, temporary or permanent withdrawal of your right to use our Services;

11.3.2. immediate, temporary or permanent withdrawal of any posting or material uploaded to our site;

11.3.3. issue a warning to you (verbal or in writing);

11.3.4. legal proceedings against you for reimbursement of all costs on an indemnity basis (which you agree is reasonable) (including but not limited to reasonable administrative and legal costs) resulting from the breach;

11.3.5. further legal action against you;

11.3.6. disclosure of such information to law enforcement authorities as we reasonably feel is necessary;

11.4. We exclude liability for actions taken in response to breaches of this AUP. The responses described in this AUP are not limited and we may take other action we reasonably deem appropriate.

11.5. We will charge you our standard hourly rate for work resulting from any breach of the AUP together with the cost of equipment and/or material needed to:-

11.5.1. investigate or otherwise respond to any suspected violation of this AUP;

11.5.2. remedy any harm caused to us or our customers by the use of your Services in violation of this AUP;

11.5.3. respond to complaints; and

11.5.4. have our Internet Protocol numbers removed from any “blacklist”.

12. OTHER

12.1. You must have valid and current information on file with your domain name registrar for any domain hosted on our network.

12.2. You may only use IP addresses assigned to you by our staff.

12.3. You may not take any action which directly or indirectly results in any of our IP space being listed on any abuse database.

13. CHANGES TO AUP

13.1. We may revise this AUP after having given prior notice to our customers As a user of this website, you are expected to check our site from time to time to take notice of any changes we make, as they are legally binding on you within 15 days (or sooner if applicable by law) from the date of notice. Some of the provisions contained in this AUP may also be superseded by provisions or notices published on our site. In the event that the change materially adversely affects your ability to use the Services, then you can terminate your agreement with us by providing us with 30 days written notice.

14. DISCLAIMER

14.1. We are under no duty and by this AUP are not deemed to undertake a duty to monitor or police our customers’ activities and we disclaim any responsibility for any misuse (deliberate or otherwise) of our network and for any direct and/or indirect financial loss whether in contract, tort (including negligence), breach of statutory duty or otherwise for any loss of profit or consequential loss arising from any breach of this AUP