ACCEPTABLE USAGE POLICY

1. Introduction and Purpose

1.1. This Acceptable Use Policy ("AUP") applies to services taken by a Customer from any Echo Group company and is binding on any person (natural or juristic) who utilises Echo's Services. The AUP sets out in detail what forms of conduct Echo regards as unacceptable on the part of its Customers and the steps which Echo may take in response to unacceptable use of its Services. Please take the time to fully acquaint yourself fully with the provisions of this Policy. Kindly direct any queries to info@echotel.international

1.2. By contracting with Echo or otherwise utilising Echo's Services, the Customer agrees, without limitation or qualification, to be bound by this AUP, the terms and conditions of the Echo Contract or Master Service Agreement (including any annexures thereto), as well as any additional service terms in associated with the Services which are imposed by Echo's suppliers.

1.3. Echo reserves the right to amend this AUP in its sole discretion, provided that such discretion is exercised in a reasonable manner.

1.4. The purpose of this AUP is to, without limitation:

1.4.1. ensure compliance with all applicable laws in the use of the Services;

1.4.2. set out the activities and online behaviour which is considered an unacceptable use of Services;

1.4.3. protect the integrity of Echo and its supplier's/sub-contractor's networks; and

1.4.4. set out the consequences which may flow as a result of engaging in such prohibited activities.

1.4.5. Echo respects the rights of Customer, and users of Echo's services, to freedom of speech and expression, access to information, privacy, human dignity, religion, belief and opinion.

2. Abuse

2.1. The Services may only be used for lawful purposes and activities. Echo prohibits any use of its Services including the transmission, storage and distribution of any material or offensive content using Echo's Services/network that violates associated laws or regulations of a country.

2.2. Customers or users are prohibited from using the Services or otherwise publishing, downloading, uploading, storing, transmitting or distributing any material or offensive content over or via Echo's network or equipment which: -

2.2.1. violates any local and international laws, including, inter alia, the laws prohibiting child pornography, obscenity, discrimination (including racial, gender or religious slurs) and hate speech, or speech designed to incite violence or hatred, or threats to cause bodily harm;

2.2.2. constitutes defamation, abuse, stalking, harassment or physically threats of any individual; including any attempt to link to, post, transmit or otherwise distribute any inappropriate or defamatory material;

2.2.3. harms or attempts to harm a minor, including, but not limited to, child pornography and cyber bullying;

2.2.4. violates any Intellectual Property laws including materials protected by local and international copyright, trademarks and trade secrets;

2.2.5. violates another's right to privacy, including any effort to collect personal data of third parties without their consent;

2.2.6. constitutes fraudulent activity, including dubious financial practices, such as pyramid schemes; the impersonation of another client without their consent; or any attempt to enter into a transaction with Echo on behalf of another customer without their consent;

2.2.7. constitutes a violation of any exchange control laws;

2.2.8. engages in any activity that results in the sale, transmission or distribution of pirated or illegal software;

2.2.9. fosters, and/or promotes any illegal, abusive, or unethical behaviour;

2.2.10. attempts to gain unauthorised 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 authorisation in writing of the owner of said data, systems or networks;

2.2.11. monitors data or traffic on any network or system without the express authorization of the owner of the said network or system;

2.2.12. interferes with any other users' network service, whether said services be provided by Echo or any other

Annexure 3 – Echo SP SA (Pty) Ltd – AUP

network, by, inter alia, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

2.2.13. uses an Internet account and/or computer without the owner's authorization;

2.2.14. collects or uses email addresses, screen names or other identifiers, without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting);

2.2.15. collects or utilises any information without the consent of the owner of the information;

2.2.16. uses any false, misleading, or deceptive TCP-IP packet header information in an email or a newsgroup posting;

2.2.17. uses the Service to distribute software that covertly gathers information about a user or covertly transmits information about the user;

2.2.18. creates a risk to a person's safety or health; creates a risk to public safety or health; compromises national security; or interferes with an investigation by law enforcement;

2.2.19. improperly exposes trade secrets or other confidential or proprietary information of another person;

2.2.20. defeats/infringes on other persons' copyrights or is intended to assist others in defeating technical copyright protections

2.2.21. promotes illegal drugs, violates export control laws, relates to illegal gambling, or illegal arms trafficking;

2.2.22. uses the Service for distribution of advertisement delivery software unless otherwise expressly consented to by the intended recipient; and/or

2.2.23. may result in action against the Echo's network or website, or Echo's Directors, employees, officers or other agents, including engaging in behaviour that results in any server being the target of a denial-of-service attack (DoS).

2.3. For purposes of this AUP, content which is published or transmitted via Echo's network or equipment includes, inter alia, web content, emails, bulletin board postings, chat, tweets, social media posts and any other type of posting or transmission that relies on the Internet.

3. Electronic mail requirements and Bulk Electronic Communications

3.1. In the event that Customer utilises Echo's Services, IP addresses or internet connection to send outbound Emails, Customer:

3.1.1. shall not send unsolicited bulk mail for marketing or any other purposes (political, religious or commercial) to people who have not consented to receiving such mail;

3.1.2. shall not use any part of Echo's infrastructure for the purpose of unsolicited bulk mail, whether sending, receiving, bouncing, or facilitating such mail;

3.1.3. shall not operate or maintain mailing lists, without the express permission of all recipients listed;

3.1.4. shall promptly remove from lists, invalid or undeliverable addresses or addresses of unwilling recipients or a recipient who have indicated that he/she wishes to be removed from such list;

3.1.5. shall not use Echo's Service(s) to collect responses from unsolicited email sent from accounts on other Internet hosts or e-mail services that violate this AUP or the AUP of any other Internet service provider; and

3.1.6. shall not use Echo's name in the header or by listing an IP address that belongs to Echo in any unsolicited email whether sent through Echo's network or not.

3.2. Customer must take steps to secure its mail server against public relay as a protection to themselves and the broader Internet community. Public relay occurs when a mail server is accessed by a third party from another domain and utilised to deliver mails, without the authority or consent of the owner of the mail-server. Mail servers that are unsecured against public relay often become abused by unscrupulous operators for spam delivery and upon detection such delivery must be disallowed.

4. Threats to Network Security

4.1. Any activity which threatens the functioning, security and/or integrity of Echo or its suppliers' networks is prohibited, including:

4.1.1. any efforts to attempt to gain unlawful and unauthorised access to the network or circumvent any of the security measures established by Echo for this goal;

4.1.2. any effort to use Echo's equipment to circumvent the user authentication or security of any host, network or account ("cracking" or "hacking");

4.1.3. forging of any TCP/IP packet headers (spoofing) or any part of the headers of an email or a newsgroup posting;

4.1.4. any effort to breach or attempt to breach the security of

another user or attempt to gain access to any other person's computer, software, or data without the knowledge and consent of such person;

4.1.5. any activity which threatens to disrupt the Services through "denial of service attacks"; flooding of a network, or overloading a service or any unauthorised probes ("scanning" or "nuking") of others' networks;

4.1.6. any activity which in any way threatens the security of the network by knowingly posting, transmitting, linking to or otherwise distributing any information or software which contains a virus, trojan horse, worm, malware, botnet or other harmful, destructive or disruptive component;

4.1.7. any unauthorised monitoring of data or traffic on the network without Echo's explicit written consent;

4.1.8. running services and applications with known vulnerabilities and weaknesses, e.g., insufficient anti-automation attacks, any traffic amplification attacks, including recursive DNS attacks, SMTP relay attacks;

4.1.9. failing to respond adequately to a denial-of-service attack (DOS / DDOS); and/or

4.1.10. attempting to probe, scan, penetrate or test the vulnerability of any Echo system or network, or to breach Echo's security or authentication measures, whether by passive or intrusive means, unless the Customer has obtained prior written consent from Echo.

5. Users Outside South Africa

Regardless of which country a user resides in, permanently or temporarily, such user will be subject to the laws of the country in which he/she is currently resident and which apply to the user. On presentation of a legal order to do so, or under obligation through an order for mutual foreign legal assistance, Echo will assist foreign law enforcement agencies in the investigation and prosecution of a crime committed using Echo's resources, including the provisioning of all personal identifiable data**.**

6. Copyrighted Material

6.1. The Customer shall not use Echo's network or services to download, publish, distribute, or otherwise copy or use in any manner any text, music, software, art, image, or other work protected by copyright law unless:

6.1.1. the Customer has been expressly authorised by the owner of the copyright to copy the work in such manner; or

6.1.2. the Customer is otherwise permitted by established copyright law to copy the work in such manner.

7. Shared Systems

The Customer shall not use any shared system provided by Echo in a way that unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of the resources of the system. For example: Echo may prohibit the automated or scripted use of Echo's Email service if same may have a negative impact on the Email system, or, alternatively, Echo may require the Customer to repair coding abnormalities in the Customers Cloud-hosted code in circumstances where it unnecessarily conflicts with other Cloud customers' use of the Cloud. The Customer accepts that Echo may quarantine or delete any data stored on a shared system if the data is infected with a virus, or is otherwise corrupted, and has the potential to infect or corrupt the Customer's system or other customers' data that is stored on the same system.

8. User Responsibilities

8.1. Customers are responsible for any misuse of Echo's Services that occurs through the Customer's account. It is the Customer's responsibility to ensure that unauthorised persons do not gain access to or misuse Echo's Services.

8.2. Where the Customer has authorised a minor to use any of the Echo's Services or access its websites, the Customer acknowledges that it is fully responsible for: the online conduct of such minor, controlling the minor's access to and use of any services or websites, and the consequences of any misuse by the minor.

8.3. In order to adopt the requirements of this AUP, the Customer undertakes to –

8.3.1. have valid and current information on file with the domain name registrar for any domain hosted on the Echo network;

8.3.2. accept that if Echo's IP numbers assigned to the Customer's account, are listed on an abuse database, the Customer will be in violation of this AUP with the result that Echo may take reasonable action to protect its IP numbers, including the suspension of service being rendered to the Customer, regardless of whether the IP numbers were listed as a result of the Customer's actions;

8.3.3. comply, at all times, with any rules, procedures and/or policies, applicable to the network and/or services, which may be updated from time-to-time, and will be provided and/or made available to Customer upon

request; and

8.3.4. accept that if the Customer should register a DNS record or zone on Echo's managed or operated DNS servers or services for a domain of which the Customer is not the registered or administrative contact according to the registrar's WHOIS system, then upon request from the registered or administrative contact Echo may modify, transfer, or delete such records or zones.

9. Breach of AUP

9.1. Upon receipt of a complaint, or having become aware of an incident, Echo may, in its sole and reasonably exercised discretion take any of the following steps:

9.1.1. treat such breach as a breach of the MSA and may suspend or terminate the Service as provided for in the MSA; and/or

9.1.2. warn the Customer, suspend the Customer account and/or revoke or cancel the Customer's Service access privileges completely; and/or

9.1.3. in the case of an abuse emanating from a third party, inform the third party's network administrator of the incident and request the network administrator or network owner to address the incident in terms of this AUP; and/or

9.1.4. suspend access of the third party's entire network until abuse can be prevented by appropriate means; and/or

9.1.5. charge the offending parties for administrative costs as well as for machine and human time lost due to the incident; and/or

9.1.6. assist other networks or website administrators in investigating credible suspicions of any activity listed in this AUP; and/or

9.1.7. institute civil or criminal proceedings; and/or

9.1.8. share information concerning the incident with other Internet access providers, or publish the information, and/or make available the users' details to law enforcement agencies; and/or

10. General

10.1.1. Echo reserves the right to take action against any individuals, companies or organisations that violate the AUP, or engage in any illegal or unlawful activity while accessing Echo's Services, to the fullest extent of the law.

10.1.2. Echo reserves the right, at its sole discretion, to act against other types of abuse not listed in this document and to investigate or prevent illegal activities being committed over Echo's network.

10.1.3. Echo does not waive its right to enforcement of this AUP at any time, or prejudice its right to take subsequent action, should Echo fail, neglect or elect not to enforce a breach of the AUP at any time.

10.1.4. Echo may vary the terms of this AUP from time-to-time, in its sole discretion.