ACCEPTABLE USE POLICY

This Acceptable Use Policy ("**AUP**") specifies the actions prohibited to users of the network and systems ("infrastructure") of GlobalMSP (Pty) Ltd ("MSP"). Users are required to adhere to this policy without exception. The terms "User", "Subscriber" and "Customer" are used interchangeably.

1. STATUS AND APPLICATION OF THIS POLICY

1.1 This AUP forms part of, and is incorporated by reference into, the agreement between MSP and the customer for the provision of services. Where there is a conflict between this AUP and the customer's service agreement, this AUP prevails in respect of permitted and prohibited use of the infrastructure. Breach of this AUP is a material breach of the customer's service agreement.

1.2 The customer is responsible for all use of the services under its account, including use by its employees, contractors, end-users, resellers and any other person to whom it provides access, and must ensure that each of them complies with this AUP.

1.3 MSP may amend this AUP from time to time. The current version will be published on MSP's website, and an amendment takes effect 20 business days after publication, except where an earlier effective date is necessary to protect the network or to comply with law.

1.4 Version: V1 | Effective date: 202608 | Approved by: Legal |Next review: 08/2027

2. LAWS AND REGULATIONS

2.1 MSP's infrastructure may be used only for lawful purposes. Users may not use the infrastructure in violation of any law or regulation applicable to them, including the laws of the Republic of South Africa and, where the user is located or operates outside South Africa, the laws of that jurisdiction. Compliance with the law of another jurisdiction does not excuse non-compliance with South African law. This AUP is governed by and interpreted in accordance with the laws of the Republic of South Africa.

2.2 Transmission, distribution or storage of any material on or through the infrastructure in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secrets or other intellectual property right used without proper authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

3. THE NETWORK

3.1 The user acknowledges that MSP is unable to exercise control over the content of the information passing over the infrastructure and the Internet, including any websites, electronic mail transmissions, news groups or other material created or accessible over its infrastructure. Therefore, MSP is not responsible for the content of any messages or other information transmitted over its infrastructure. MSP acts as a mere conduit, cache and host in respect of such content and relies on the limitations of liability afforded to service providers under Chapter XI of the Electronic Communications and Transactions Act 25 of 2002. MSP does not monitor content and is under no general obligation to do so, but will act on a valid take-down notification in accordance with the take-down procedure set out in this AUP.

3.2 MSP's infrastructure may be used to link into other networks worldwide and the user agrees to conform to the acceptable use policies of these networks.

3.3 The user may obtain and download any materials marked as available for download off the Internet but is not permitted to use its Internet access to distribute any copyrighted materials unless permission for such distribution is granted to the user by the owner of the materials.

3.4 The user is prohibited from obtaining and/or disseminating any unlawful materials, including but not limited to stolen intellectual property, child sexual abuse material, material that constitutes unlawful hate speech, and material that is prohibited or has been refused classification under the Films and Publications Act 65 of 1996. MSP will report child sexual abuse material to the South African Police Service and preserve the associated evidence as required by law and will suspend the account concerned with immediate effect.

4. SYSTEM AND NETWORK SECURITY

4.1 All references to systems and networks under this section includes the Internet (and all those systems and/or networks to which user is granted access through MSP) and includes but is not limited to the infrastructure of MSP itself.

4.2 The user may not circumvent user authentication or security of any host, network, or account (referred to as “cracking” or “hacking”), nor interfere with service to any user, host, or network (referred to as “denial of service attacks”).

4.3 Violations of system or network security by the user are prohibited and may result in civil liability and criminal prosecution, including under the Cybercrimes Act 19 of 2020. MSP will investigate incidents involving such violations and will co-operate with law enforcement officials if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

4.3.1 Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of any system or network or to breach security or authentication measures without the express authorisation of MSP.

4.3.2 Unauthorised monitoring of data or traffic on the network or systems without express authorisation of MSP.

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

4.3.4 Forging of any TCP/IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting.

5. PROHIBITED NETWORK AND SYSTEM USES

5.1 The user may not use the infrastructure to create, host, distribute or control malware, ransomware, botnets or command-and-control infrastructure, or to conduct phishing, pharming, identity theft or any other fraudulent activity.

5.2 The user may not operate insecure or misconfigured services that facilitate abuse, including open mail relays, open DNS resolvers, open proxies and unpatched or unmanaged connected devices, and must remediate any such condition promptly on notification by MSP.

5.3 The user may not use the services for cryptocurrency mining or any other activity that consumes network, processing or storage resources disproportionately to the service purchased, without MSP's prior written consent.

6. FAIR ACCESS POLICY

6.1 To help ensure that all users have fair and equal use of the service and to protect the integrity of the network, MSP reserves the right, and will take necessary steps, to prevent improper or excessive usage thereof, the action that MSP may take includes, but is not limited to:

6.1.1 Limiting throughput

6.1.2 Preventing or limiting service through specific ports or communication protocols; and/or

6.1.3 Complete termination of service to users who grossly abuse the network through improper or excessive usage.

6.2 This policy applies to and will be enforced for intended and unintended (e.g., viruses, worms, malicious code, or otherwise unknown causes) prohibited usage.

6.3 Online activity will be subject to the available bandwidth, data storage and other limitations of the service provided, which MSP may revise from time to time on reasonable notice to the customer. Where a revision materially and adversely affects the customer, MSP will give at least 20 business days' written notice and the customer may terminate the affected service without penalty before the revision takes effect. MSP may implement changes without prior notice only where necessary to protect the integrity or security of the network, in which case notice will be given as soon as reasonably practicable.

7. VOICE, NUMBERING AND TELECOMMUNICATIONS FRAUD

7.1 The user may not use the services to commit or facilitate telecommunications fraud, including subscription fraud, toll fraud, compromise of PBX or SIP trunking facilities, artificially inflated traffic, international revenue share fraud, or the use of SIM boxes or any other means of bypassing licensed international gateways or interconnection arrangements.

7.2 The user may not transmit inaccurate, misleading or spoofed calling line identification, may not use numbering resources otherwise than in accordance with the applicable national numbering plan and ICASA regulations, and may not resell or otherwise make available voice services except as expressly permitted in writing by MSP.

7.3 The user is responsible for securing its PBX, SIP credentials and endpoint equipment, and remains liable for all charges arising from traffic originated on its account, including traffic resulting from the compromise of its equipment or credentials, except to the extent that the compromise is attributable to MSP.

8. EMAIL USE

8.1 It is explicitly prohibited to send unsolicited bulk mail messages (“junk mail” or “spam”) of any kind (commercial advertising, political tracts, announcements, etc.). This is strongly objected to by most Internet users, and the repercussions against the offending party and MSP can result in disruption of service to other users connected to MSP. The user may not forward or propagate chain letters or malicious email; send multiple unsolicited electronic mail messages, or engage in “mail-bombing” of one or more recipients; send bulk electronic messages without identifying, within the message, a reasonable means of opting out of further messages from the sender; use redirect links in unsolicited commercial email to advertise a website or service; operate or support any address-harvesting, list-washing or dictionary-attack service; or send electronic communications in contravention of the direct marketing requirements of the Protection of Personal Information Act 4 of 2013 or the Consumer Protection Act 68 of 2008.

8.2 Maintaining of mailing lists by users of MSP is accepted only with the permission and approval of the list members, and at the members’ sole discretion. Should mailing lists contain invalid or undeliverable addresses or addresses of unwilling recipients those addresses must be promptly removed.

8.3 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. Users’ mail servers must be secure against public relay as a protection to both themselves and the Internet at large. 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. MSP reserves the right to examine users’ mail servers to confirm that no mails are being sent from the mail server through public relay and the results of such checks can be made available to the user. MSP also reserves the right to examine the mail servers of any users using MSP mail servers for “smarthosting” (when the user relays its mail off an MSP mail server to a mail server of its own) or similar services at any time to ensure that the servers are properly secured against public relay. All relay checks will be limited to what is necessary to verify that the server is secured against public relay, will not involve inspection of the content of communications, and will be conducted

in accordance with MSP's Privacy Policy, the Protection of Personal Information Act 4 of 2013 and the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002. By using the service the user consents to such checks.

9. TAKE-DOWN NOTIFICATION

9.1 MSP is a member of the Internet Service Providers' Association (ISPA), a recognised industry representative body, and has adopted its code of conduct. Any person who alleges that data hosted or transmitted on MSP's infrastructure infringes their rights may lodge a take-down notification meeting the requirements of section 77 of the Electronic Communications and Transactions Act 25 of 2002.

9.2 Take-down notifications must be directed to MSP's designated agent, in the form and in accordance with the procedure published on MSP's website. A notification that does not meet the statutory requirements will not be actioned.

9.3 MSP will act on a valid take-down notification without undue delay. Removal of, or disabling access to, data under this section is without prejudice to any other right or defence available to MSP and does not constitute an admission of liability. A person who lodges a materially false or misleading take-down notification may be liable for damages under section 77(2) of that Act.

10. COMPLAINTS

10.1 Upon receipt of a complaint, or having become aware of an incident, MSP reserves the right to:

10.1.1 Inform the user’s network administrator of the incident and require the network administrator or network owner to deal with the incident according to this AUP.

10.1.2 In the case of individual users suspend the user’s account and withdraw the user’s network access privileges completely.

10.1.3 Recover from the offending party MSP's reasonable costs of investigating and remedying the incident, including administrative costs and machine and human time, supported by an itemised statement of those costs.

10.1.4 In severe cases suspend access of the user’s entire network until abuse can be prevented by appropriate means.

10.1.5 Share information concerning the incident with other electronic communications service providers, industry abuse-handling bodies and law enforcement agencies, where lawful and necessary to prevent or address abuse. Any processing or disclosure of personal information under this AUP will be carried out in accordance with the Protection of Personal Information Act 4 of 2013. MSP will not publish the personal information of a user in connection with an incident except where required by law or by order of a competent court or regulator.

10.2 MSP may take any one or more of the steps listed above, applying the step or steps that are reasonably proportionate to the nature and severity of the incident. Except where immediate action is necessary to protect the network, other users or any person's safety, or where required by law, MSP will notify the user of the incident and allow a reasonable opportunity to remedy it before suspending or terminating the service. Where immediate action is taken, MSP will notify the user as soon as reasonably practicable and provide reasons. A user may dispute any action taken under this AUP by written notice to complaints@globalmsp,net, and MSP will review the matter and respond within 10 business days. Nothing in this AUP limits any right the user has under the Consumer Protection Act 68 of 2008, the Electronic Communications Act 36 of 2005 or ICASA's end-user and subscriber service charter regulations.

11. INDEMNITY AND GENERAL

11.1 The user indemnifies MSP against any claim, loss, damage, penalty, fine or expense (including reasonable legal costs) arising from the user's breach of this AUP or from any use of the services by the user or by any person using the user's account.

11.2 MSP is not liable for any loss suffered by the user as a result of any action lawfully taken under this AUP.

11.3 The user's obligations under this AUP, and any liability accrued under it, survive termination of the services.

11.4 If any provision of this AUP is or becomes unenforceable, that provision is severable and the remaining provisions continue in full force and effect.

12. REPORTING

12.1 All cases of violation of this Acceptable Use Policy should be reported to complaints@globalmsp.net