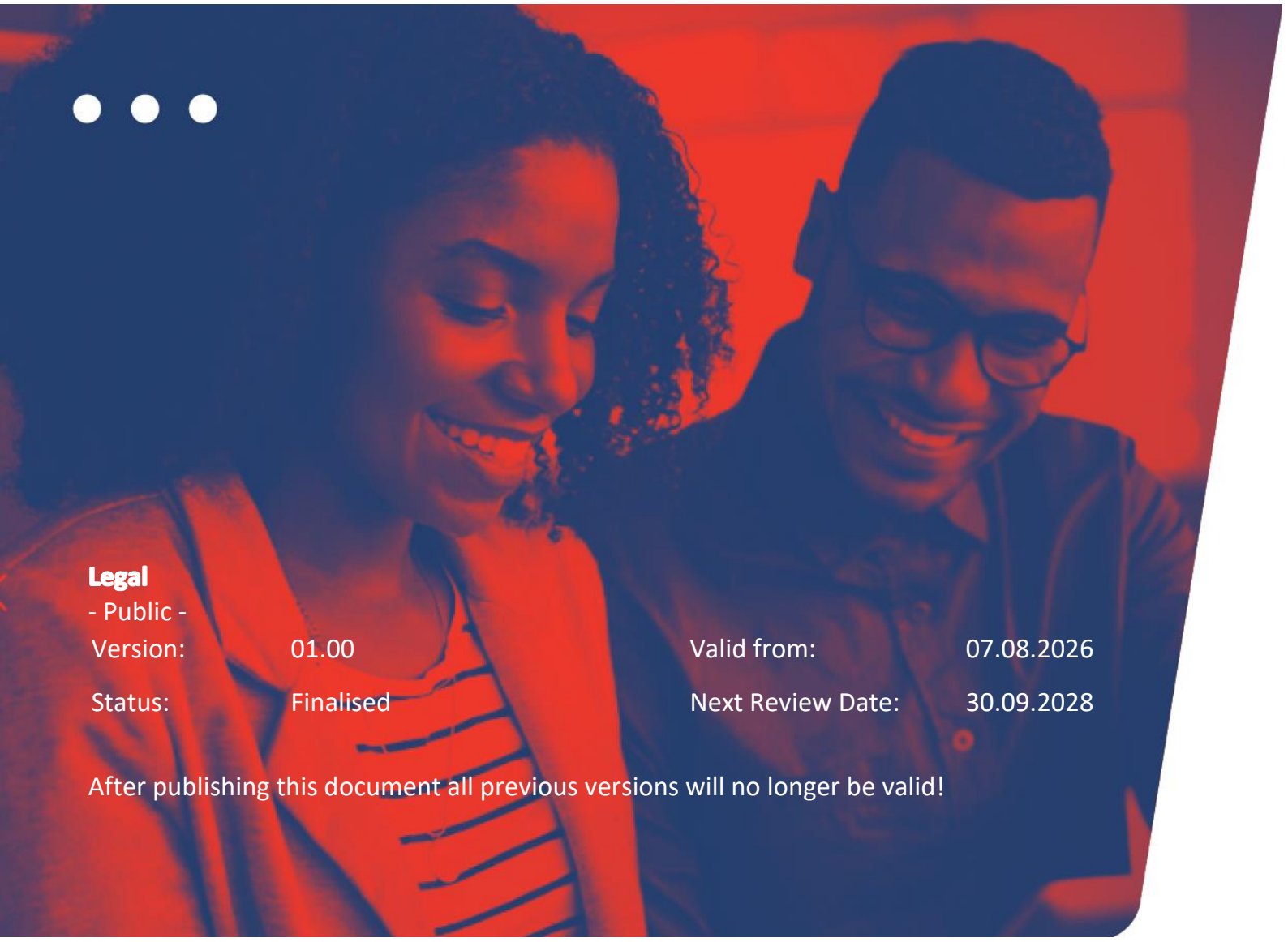
GIJ-POL-003506_INTERNET ACCEPTABLE USE POLICY

INTERNET ACCEPTABLE USE POLICY



Legal

- Public -

Version:	01.00	Valid from:	07.08.2026
Status:	Finalised	Next Review Date:	30.09.2028

After publishing this document all previous versions will no longer be valid!

Gijima

TABLE OF CONTENTS

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation
ASN	Autonomous System Number
AUP	Acceptable Use Policy
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
IP	Internet Protocol
POPIA	Protection of Personal Information Act
QMS	Quality Management System

Table 1: Abbreviations and Acronyms

GLOSSARY OF TERMS

Term	Explanation
Abuse	Any use of the Services that violates this Policy, Applicable Law, or compromises the security, integrity, or availability of the Services.

Term	Explanation
Abuse Report	A report submitted to the Company regarding suspected misuse, unlawful activity, or security incidents affecting the Services.
Botnet	A network of compromised devices controlled to perform malicious activities.
Malware	Malicious software including viruses, worms, ransomware, Trojans, and other harmful code.
Phishing	Fraudulent communications intended to deceive recipients into disclosing confidential information.
Policy	This Acceptable Use Policy, as amended from time to time.
Routing Information	Information used to direct network traffic across interconnected networks.
Security Incident	An event involving unauthorised access, misuse, compromise, disruption, or attempted compromise of systems, networks, or Services.
Spam	Unsolicited bulk electronic communications.

Table 2: Glossary of Terms

1 INTERPRETATION AND DEFINITIONS

In this Policy, unless the context indicates otherwise, the following words and expressions shall bear the meanings assigned to them and cognate expressions shall bear corresponding meanings:

(a) Agreement means the agreement governing the provision of the Services between the Company and the Customer, together with all schedules, service orders, service descriptions, annexures and documents incorporated by reference.
(b) Applicable Law means all legislation, regulations, regulatory directives, licences, industry codes, court orders and other legal requirements applicable to the provision or use of the Services in the Republic of South Africa.
(c) Company means Gijima Holdings (Pty) Ltd and/or the applicable Gijima group company providing the Services under the Agreement.
(d) Customer means the person or legal entity contracting directly with the Company for the provision of the Services.
(e) End User means any person or entity who accesses or uses the Services through or on behalf of the Customer, including the Customer's employees, contractors, consultants, agents, affiliates, customers or any other authorised users.
(f) Policy means this Acceptable Use Policy, as amended from time to time in accordance with its terms and the Agreement.
(g) Services means the electronic communications, Internet connectivity, hosting, cloud, managed network, data centre, security, voice and any other related services provided by the Company under the Agreement.
(h) Unless the context indicates otherwise:
    i. references to the singular include the plural and vice versa;
    ii. references to one gender include the other genders;
    iii. headings are included for convenience only and do not affect interpretation;
    iv. a reference to any legislation includes any amendment, replacement or re-enactment thereof.

2 PURPOSE

The purpose of this Policy is to establish the acceptable use requirements applicable to Customers making use of the Services.

This Policy is intended to:

(a) protect the security, integrity, availability and reliability of the Company's network and Services;
(b) promote the lawful, secure and responsible use of the Services;
(c) protect Customers, End Users and third parties from unlawful, fraudulent or harmful conduct;
(d) support compliance with Applicable Law and recognised industry standards; and
(e) minimise operational, legal and cybersecurity risks associated with the use of the Services.

This Policy forms part of the Agreement and must be read together with the Agreement and any other policies expressly incorporated therein.

In the event of any inconsistency between this Policy and the Agreement, the provisions of the Agreement shall prevail unless expressly stated otherwise.

The Company may amend this Policy from time to time where reasonably necessary to reflect changes in Applicable Law, regulatory requirements, operational practices, industry standards, security threats or the Services offered. Any such amendment shall take effect in accordance with the Agreement and Applicable Law.

3 SCOPE

This Policy applies to every Customer making use of the Services provided by the Company.

The Customer remains responsible for ensuring that all End Users comply with this Policy.

The Customer acknowledges that any use of the Services by an End User shall, for purposes of this Policy, be deemed to be use by the Customer.

The Customer shall take reasonable contractual, administrative and technical measures to ensure compliance with this Policy by all persons making use of the Services through the Customer.

Nothing contained in this Policy prevents the Customer from implementing additional acceptable use requirements applicable to its End Users, provided that such requirements do not conflict with or reduce the protections afforded to the Company under this Policy.

4 CUSTOMER RESPONSIBILITIES

The Customer shall:

(a) ensure that its own use of the Services, and the use of the Services by its End Users, complies with this Policy and Applicable Law;
(b) not knowingly permit or facilitate the use of the Services for any unlawful, fraudulent or malicious purpose;
(c) implement and maintain reasonable administrative, organisational, physical and technical safeguards appropriate to the nature of the Services utilised;
(d) maintain reasonable security controls over all devices, systems and infrastructure connected to the Services;
(e) apply appropriate security updates and patches to systems connected to the Services where reasonably necessary to mitigate known security vulnerabilities;
(f) promptly investigate any suspected compromise of systems connected to the Services;
(g) notify the Company without undue delay upon becoming aware of any security incident, unauthorised access, unlawful activity or material misuse of the Services that may affect the Company, its network or other Customers;
(h) cooperate reasonably with the Company during any investigation into suspected abuse or misuse of the Services;
(i) ensure that all information supplied to the Company relating to the provision of the Services remains accurate and up to date;
(j) remain responsible for all activity originating from or occurring through the Services supplied to the Customer, whether such activity is undertaken by the Customer, its employees, contractors, agents, affiliates, resellers or End Users; and
(k) comply with all reasonable operational, technical and security requirements communicated by the Company from time to time where necessary to protect the integrity, security or availability of the Services.

5 PROHIBITED USE

The Customer shall not use, or permit any End User to use, the Services to:

(a) contravene any Applicable Law;
(b) commit, facilitate or attempt to commit fraud, theft, identity theft, deception or any other unlawful conduct;
(c) infringe, misappropriate the intellectual property rights, or other proprietary rights of any person;

(d) publish, store, transmit or otherwise make available any content that is unlawful or that the Customer is not legally entitled to distribute;
(e) impersonate any person, organisation, communications service or network;
(f) misrepresent the source, origin or identity of electronic communications or network traffic;
(g) interfere with another person's lawful use or enjoyment of any electronic communications service, information system or communications network;
(h) intentionally interfere with, disrupt or impair the operation, security or availability of any communications network or information system;
(i) engage in conduct that is reasonably likely to damage the reputation, integrity or lawful operation of the Company's Services; or
(j) knowingly use the Services in any manner that exposes the Company or other Customers to material legal, operational or cybersecurity risk.

6 NETWORK AND SECURITY ABUSE

The Customer shall not use, or permit any End User to use, the Services to:

(a) gain, or attempt to gain, unauthorised access to any computer system, communications network, application, account or electronic service;
(b) perform password guessing, credential stuffing, brute-force authentication attempts or any similar activity intended to compromise the confidentiality, integrity or availability of any system;
(c) conduct vulnerability assessments, penetration testing, port scanning, network scanning or similar security testing against any third-party systems without the prior written authorisation of the owner of those systems;
(d) introduce, distribute, host or facilitate the distribution of malware, ransomware, viruses, worms, Trojan software or any other malicious code;
(e) establish, operate or participate in any botnet, malicious command-and-control infrastructure or other malicious network activity;
(f) launch, facilitate or participate in any denial-of-service (DoS), distributed denial-of-service (DDoS) or similar attack intended to impair the availability of any network, system or service;
(g) perform amplification, reflection or other attacks intended to generate excessive network traffic or disrupt communications services;
(h) falsify, spoof or manipulate Internet Protocol addresses, routing information, domain name system (DNS) records, packet headers or other network identifiers in a manner intended to deceive, conceal identity or interfere with network operations;
(i) intercept, monitor or capture electronic communications except where authorised by Applicable Law; or
(j) interfere with, bypass or attempt to circumvent security controls implemented by the Company.

7 EMAIL, MESSAGING AND COMMUNICATIONS

The Customer shall not use, or permit any End User to use, the Services to:

(a) transmit unsolicited bulk electronic communications, commonly referred to as spam;
(b) operate, facilitate or support unsolicited email, messaging or marketing campaigns in contravention of Applicable Law;
(c) distribute phishing communications, fraudulent electronic messages or any communication intended to deceive recipients into disclosing confidential information;
(d) forge or falsify email headers, sender identities, message routing information or other communication metadata;
(e) knowingly operate open mail relays, insecure messaging infrastructure or other systems that facilitate abuse of electronic communications services;

(f) engage in mail bombing, excessive automated messaging or other communications activity that materially impairs the operation of the Company's Services or those of third parties; or
(g) use the Services in a manner that causes the Company or its Internet Protocol address space to be listed on recognised spam or abuse blacklists.

8 HOSTING, CONTENT AND APPLICATION SERVICES

The Customer remains solely responsible for all content created, stored, transmitted, processed or made available through the Services.

The Customer shall not host, distribute or facilitate the operation of malicious software, infrastructure or services intended to facilitate cybercrime or other unlawful activity.

The Customer shall not knowingly host phishing websites, credential harvesting platforms, fraudulent online services or other infrastructure designed to deceive users.

The Customer shall not distribute software or applications designed primarily to compromise, disrupt or obtain unauthorised access to computer systems or electronic communications networks.

The Customer shall not use the Services to store, publish or distribute material that is unlawful or infringes the rights of any third party.

Where the Company reasonably believes that hosted content or applications present a material risk to the security, integrity or availability of the Services, the Company may suspend, isolate or restrict access to the affected Services in accordance with clause **11 INVESTIGATIONS AND ABUSE MANAGEMENT**.

9 FAIR, RESPONSIBLE AND REASONABLE USE

The Customer shall use the Services in a manner that does not materially impair the performance, security or availability of the Company's network or Services.

The Customer shall not intentionally consume shared network resources in a manner that unfairly or materially impacts other customers or users of the Company's network.

The Customer shall not circumvent or attempt to circumvent service limitations, traffic management mechanisms, bandwidth controls or security measures implemented by the Company.

The Company may implement reasonable traffic engineering, congestion management, rate limiting, filtering, mitigation measures or other operational controls where reasonably necessary to:

(a) preserve the integrity, security or availability of the Services;
(b) respond to security incidents or network abuse;
(c) protect other customers or third parties; or
(d) comply with Applicable Law or regulatory requirements.
(e) Nothing contained in this Policy prevents the Company from taking immediate action where reasonably necessary to protect the security, integrity or availability of its network or Services.

10 WHOLESALE SERVICES AND CUSTOMER OBLIGATIONS

Customers utilising dedicated Internet access, IP transit, peering, wholesale connectivity or other enterprise networking Services shall operate their networks in accordance with generally accepted Internet operational practices.

The Customer shall not advertise, originate or propagate Internet routing information unless authorised to do so.

The Customer shall implement and maintain appropriate routing policies and technical controls to minimise the risk of route leaks, route hijacking, routing instability or degradation of Internet connectivity.

The Company may implement routing filters, prefix limits, route validation, security controls or other reasonable technical measures to protect its network and interconnected communications networks.

Where Internet numbering resources, including Internet Protocol addresses or Autonomous System Numbers, are allocated to the Customer by or through the Company, such resources shall be used only for their intended purpose and in accordance with applicable registry policies.

The Customer shall cooperate with the Company in investigating and resolving routing anomalies, network incidents or abuse affecting the Services.

Where the Customer resupplies or makes the Services available to third parties, the Customer shall ensure that its agreements with those third parties impose acceptable use obligations substantially equivalent to those contained in this Policy.

11 INVESTIGATIONS AND ABUSE MANAGEMENT

The Company may investigate any actual or suspected breach of this Policy.

In conducting any investigation, the Company may collect, preserve, review and disclose information reasonably necessary to investigate suspected abuse, unlawful activity or security incidents, subject to Applicable Law, including applicable data protection and privacy legislation.

The Customer shall provide all reasonable assistance requested by the Company in connection with any investigation relating to the Services.

Where reasonably necessary, the Company may communicate and cooperate with upstream or downstream service providers, Internet exchange operators, recognised cybersecurity organisations, regulatory authorities and law enforcement agencies for the purposes of investigating, preventing or mitigating network abuse or unlawful activity.

Nothing contained in this Policy requires the Company to delay any action where immediate intervention is reasonably necessary to protect the security, integrity or availability of the Services or the Company's network.

12 ENFORCEMENT

Where the Company reasonably believes that the Customer or an End User has breached this Policy, or that continued use of the Services poses a material risk to the Company's network, Services, Customers or third parties, the Company may take such action as it reasonably considers necessary to protect its legitimate interests.

Without limiting any rights available to the Company under the Agreement or Applicable Law, the Company may:

(a) issue a written warning;
(b) require the Customer to investigate and remedy the breach within a reasonable period;
(c) require the Customer to remove or disable access to offending content, applications or systems;
(d) temporarily restrict, suspend or limit access to all or part of the Services;
(e) block or filter specific traffic, protocols, Internet Protocol addresses or other network activity reasonably associated with the breach;
(f) isolate or disconnect compromised systems from the Company's network;
(g) report suspected unlawful conduct to the appropriate regulatory authority or law enforcement agency; and/or

(h) terminate the affected Services or the Agreement where the breach is material, repeated or incapable of remedy.

Where reasonably practicable, the Company shall notify the Customer before taking action under this clause. The Company may, however, act without prior notice where immediate action is reasonably necessary to protect the security, integrity or availability of the Services or to comply with Applicable Law.

The Company's exercise of any rights under this Policy shall not constitute a waiver of any other rights or remedies available under the Agreement, Applicable Law or at common law.

Subject to the Agreement and Applicable Law, the Company shall not be liable for any loss, damage or interruption arising from any suspension, restriction or other action reasonably taken in accordance with this Policy.

13 LIABILITY AND INDEMNITY

The Customer remains responsible for all activity originating from or occurring through the Services supplied to the Customer, regardless of whether such activity is undertaken by the Customer or by any End User.

Except to the extent expressly provided otherwise in the Agreement or prohibited by Applicable Law, the Company shall not be responsible for:

(a) content created, stored, transmitted or received by the Customer or any End User;
(b) the accuracy, legality or reliability of any information transmitted using the Services;
(c) any unlawful or unauthorised use of the Services by the Customer or any End User; or
(d) any loss arising from the Customer's failure to comply with this Policy.
(e) Subject to Applicable Law and the limitations of liability contained in the Agreement, the Customer indemnifies and holds harmless the Company, its directors, employees and agents against all claims, losses, damages, liabilities, costs and expenses (including reasonable legal costs) arising from:
(f) the Customer's breach of this Policy;
(g) any unlawful or negligent use of the Services by the Customer or its End Users; or
(h) any third-party claim arising from the Customer's use of the Services.
(i) Nothing contained in this Policy excludes or limits any liability that cannot lawfully be excluded or limited under Applicable Law.

14 REPORTING ABUSE

Suspected abuse of the Services may be reported using the Company's published abuse reporting channels.

Abuse reports should, where reasonably available, include sufficient information to enable investigation, including:

(a) the date and time of the incident;
(b) the affected Internet Protocol address or domain name;
(c) relevant system logs or supporting evidence;
(d) a description of the suspected abuse; and
(e) any other information reasonably required to investigate the matter.

The Company may request additional information where reasonably necessary to investigate or resolve a reported incident.

The Company reserves the right to determine the priority, manner and timeframe within which abuse reports are investigated, having regard to the nature, severity and potential impact of the reported activity.

15 GENERAL PROVISIONS

This Policy shall be governed by and interpreted in accordance with the laws of the Republic of South Africa.

If any provision of this Policy is held to be invalid, unlawful or unenforceable, that provision shall, to the extent necessary, be severed from the remainder of the Policy, and the remaining provisions shall continue in full force and effect.

This Policy shall be read together with the Agreement and any documents expressly incorporated therein by reference.

Nothing contained in this Policy limits or prejudices any rights or remedies available to the Company under the Agreement, Applicable Law or at common law.

A failure or delay by the Company to enforce any provision of this Policy shall not constitute a waiver of any right or remedy.

This Policy is intended to establish minimum acceptable use requirements. Nothing in this Policy prevents the Customer from implementing more stringent acceptable use requirements for its End Users, provided that such requirements are consistent with this Policy and the Agreement.