ACCEPTABLE USE POLICY

CipherWave Business Solutions (Pty) Ltd with registration number 2002/027250/07

Version: 1.1 Effective date: 14 August 2026
Website: www.cipherwave.co.za
Abuse reports: legal@cipherwave.co.za
Take-down notices: legal@cipherwave.co.za
Information Officer: Wayne Marlon D'Sa

1. What this Policy is

1.1 This Acceptable Use Policy (**AUP** or **Policy**) sets out the rules for using services supplied by **Cipherwave** (**we**, **us**, **our**).

1.2 The purpose of this Policy is to protect our network and systems; our customers and other users; third-party networks and systems; the security, reliability and availability of our services; and our compliance with South African law.

1.3 This Policy forms part of, and must be read with, your customer agreement, service order, service level agreement, privacy notice, fair usage policy and any product-specific terms. If you have signed a written agreement with us, the order of precedence in clause 26 applies. Nothing in any agreement permits unlawful or abusive use of the services.

2. Services this Policy covers

This Policy applies to all services we supply, including (where applicable): fibre-to-the-business and broadband internet access; VoIP, SIP trunking, hosted voice and PBX services; hosting, cloud, server, co-location and storage services; email, domain, DNS and related internet services; managed network, firewall and security services; customer premises equipment and managed devices; and our portals, APIs and support platforms.

3. Who must comply

3.1 This Policy applies to you as our customer and to your directors, employees, contractors, agents, end-users, and any person who uses the services through your account, equipment, premises, credentials, network or systems.

3.2 You are responsible for all use of the services supplied to you, whether authorised or not, unless you prove that the misuse occurred solely because of our breach or fault.

4. General obligation

You must use the services responsibly and lawfully, and in a way that does not: breach any law; infringe anyone's rights; damage, overload or interfere with our network, systems or services, or those of any third party; expose us, our customers or third parties to legal, regulatory, security or reputational risk; or interfere with another user's reasonable use of the services.

5. Compliance with law

You must comply with all applicable laws, regulations, licence conditions, regulatory requirements and lawful instructions of competent authorities, including (where applicable): the Electronic Communications Act 36 of 2005 and ICASA regulations; the Electronic Communications and Transactions Act 25 of 2002; the Cybercrimes Act 19 of 2020; the Protection of Personal Information Act 4 of 2013; the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002; the Consumer Protection Act 68 of 2008; the Films and Publications Act 65 of 1996; the Copyright Act 98 of 1978 and other intellectual property laws; and all lawful court orders, warrants, preservation requests and regulatory notices.

6. Prohibited unlawful use

You may not use the services to commit, facilitate, assist, host, transmit or make available anything unlawful, including:

(a) fraud, theft, extortion, corruption or scams;
(b) phishing, spoofing, impersonation or credential harvesting;
(c) unauthorised access to any system, account, network, device or data;
(d) unlawful interception, modification, deletion, copying or disclosure of data or communications;
(e) unlawful interference with data, computer programs, systems, networks or services;
(f) creating, hosting, transmitting or distributing malware (including viruses, ransomware, spyware, worms, trojans and botnet tools);
(g) denial-of-service or distributed-denial-of-service activity;
(h) identity theft or misuse of personal information;
(i) any material or activity involving child sexual abuse material or the sexual exploitation of children;
(j) unlawful hate speech, threats, harassment, intimidation, stalking or incitement to violence;
(k) defamatory or unlawfully privacy-infringing publication;
(l) unlawful sale or promotion of controlled substances, weapons, counterfeit goods or illegal services; or
(m) any other conduct constituting an offence or delict under South African law or the law applicable where the conduct occurs.

7. Cybersecurity and network abuse

You may not use the services for security-abusive or network-abusive activity directed at our network or any third-party network, including: hacking, intrusion attempts or unauthorised penetration testing; unauthorised port or vulnerability scanning; credential stuffing or brute-force attacks; operating or participating in a botnet; deploying or distributing malware; unauthorised packet interception; spoofing IP/MAC addresses, caller identification, email headers or routing information; operating an open mail relay, open proxy or open DNS resolver liable to abuse; causing or amplifying denial-of-service attacks; evading authentication, usage limits, traffic management or security controls; or attempting to access or interfere with our systems, provisioning platforms, routers, switches or customer premises equipment without permission.

8. Email, messaging, spam and direct marketing

8.1 You may not send, relay, host or facilitate spam or unlawful unsolicited communications. In particular, you may not: send bulk or unsolicited commercial email, SMS, voice or messaging without lawful authority and the consent required by law; use harvested, scraped or unlawfully obtained lists; forge or misrepresent sender identity, headers or routing; continue sending to recipients who have opted out; operate open relays; or send communications that result in blacklisting of our IP ranges or domains.

8.2 If you send bulk communications lawfully, you must comply with applicable direct-marketing and privacy law (including section 69 of the Protection of Personal Information Act 4 of 2013), maintain proper opt-in records, identify the sender accurately, provide a working opt-out mechanism, honour opt-outs promptly, and configure your systems to accepted industry standards (including appropriate SPF, DKIM and DMARC where applicable).

9. Hosting, content and online publication

9.1 If you use our hosting, cloud, server, DNS, domain or storage services, you are responsible for all content, applications and data you host, store, publish or make available.

9.2 You may not host, store, publish or make available content that is unlawful; infringes intellectual property rights; contains child sexual abuse material; unlawfully incites violence, hatred or discrimination; is defamatory or unlawfully infringes privacy or dignity; contains malware; is used for phishing or scams; unlawfully discloses personal or confidential information; unlawfully circumvents security or copyright protection measures; or otherwise exposes us to legal, regulatory or reputational risk.

9.3 We are not obliged to pre-screen, monitor or edit customer content, and we do not do so as a general practice. We may act in accordance with this Policy, the take-down framework in the Electronic Communications and Transactions Act 25 of 2002, a court order, a lawful regulatory or enforcement request, or our contractual rights, where we become aware of alleged unlawful content or abuse.

10. Intellectual property

You may not use the services to infringe or facilitate infringement of intellectual property rights, including unlawful copying, distribution, streaming or hosting of copyright works; hosting or linking to pirated software, films, music, games or books; distributing counterfeit goods or infringing trademarks / trade marks; or unlawfully circumventing technological protection measures.

11. VoIP, PBX and voice services

11.1 If you use our VoIP, SIP, PBX or hosted voice services, you may not: make unlawful, threatening, harassing, obscene or fraudulent calls; conduct unlawful robocalling or bulk voice campaigns; spoof caller identification or misrepresent call origin; use the services for toll fraud, bypass fraud, SIM-boxing, grey routing or unlawful call termination; resell, route or terminate traffic without our written consent and any required licence or regulatory approval; interfere with numbering plans, emergency services or network integrity; or use the services in a manner that generates fraudulent, abnormal or suspicious call patterns.

11.2 You are responsible for securing your PBX, handsets, SIP trunks, credentials, firewall and network environment. You must use strong, non-default credentials and must notify us immediately if you suspect compromise, toll fraud or unauthorised use.

12. Resource usage, fair use and network integrity

12.1 You must use the services consistently with the product purchased, the agreed service description and any applicable fair usage policy (published in accordance with the ICASA End-user and Subscriber Service Charter Regulations, 2016, where applicable to your service).

12.2 You may not: use a consumer or standard business service as a wholesale, resale, mass-hosting or public-hotspot service unless expressly permitted; place abnormal or sustained load that degrades service; bypass bandwidth controls, shaping, filtering, authentication or accounting systems; manipulate usage or billing records; use IP addresses, prefixes or routing resources not assigned or authorised by us; or connect unauthorised equipment that causes interference or security risk.

12.3 We may apply reasonable and lawful network-management measures to protect service quality, security and network integrity, including traffic prioritisation, rate limiting, filtering, blocking, blackholing or suspension.

13. Resale and sharing of services

Unless your agreement expressly allows it, you may not resell, redistribute, rebrand, wholesale, share or lease the services, or use them to operate an unauthorised ISP, public Wi-Fi, carrier/transit, voice-

termination or public hosting/VPN/proxy service, unless we have approved this in writing and you hold all necessary rights, licences and approvals.

14. Your security obligations

14.1 You must take reasonable measures to secure your systems, users, credentials and data, including: using strong passwords and multi-factor authentication; securing routers, firewalls, servers, PBX systems and endpoints; applying security updates; disabling unnecessary services and default credentials; maintaining anti-malware protection; configuring mail, DNS and web services securely; and monitoring for compromise.

14.2 If we reasonably believe your system is compromised, vulnerable, misconfigured or being abused, we may require you to remediate within a specified time. In urgent cases we may suspend, isolate, filter or restrict the affected service without prior notice (see clause 21).

15. Credentials and account responsibility

You must keep all usernames, passwords, SIP credentials, API keys and administrative credentials confidential and secure. You may not share credentials except with authorised persons, use default credentials, permit unauthorised access, or access another customer's account. You must notify us immediately if credentials are lost, stolen or compromised.

16. Personal information and privacy

16.1 You must process personal information lawfully and in accordance with the Protection of Personal Information Act 4 of 2013. You may not use the services to unlawfully collect, scrape, store, sell or disclose personal information, conduct unlawful surveillance, host personal-information databases without appropriate security safeguards, or send unlawful direct marketing.

16.2 Our own processing of personal information is governed by our **Privacy Policy**, available at https://cipherwave.co.za/privacy-policy/. We may process service, traffic, billing, diagnostic, security and abuse-related information as reasonably necessary to provide the services, manage and secure our network, investigate abuse, comply with law, and enforce this Policy, on the lawful bases set out in our privacy notice.

17. Monitoring, filtering and investigation

17.1 We have no general obligation to monitor customer content or communications, and we do not do so as a general practice.

17.2 We may, to the extent reasonably necessary and lawful, monitor, access, collect, analyse, block, filter or disclose information for purposes including: operating, maintaining and securing our network and services; detecting, investigating and mitigating abuse, spam, malware, cyber incidents or network attacks; responding to support requests; ensuring service quality; complying with law, court orders, warrants, regulatory directions, preservation requests and lawful enforcement requests; enforcing this Policy; and protecting our rights, customers and network.

17.3 We will not intentionally access the content of communications except where lawfully permitted, authorised, required, or technically necessary. Any interception of communications will be conducted only in accordance with the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

18. Take-down notices and unlawful content complaints

18.1 We may receive complaints or take-down notifications alleging that content transmitted or hosted through our services is unlawful. To enable us to act, and to comply with the take-down-notification

framework in the Electronic Communications and Transactions Act 25 of 2002, a notification should be in writing and should include, as far as possible:

(a) the complainant's full name, address and contact details;
(b) the written or electronic signature of the complainant (or authorised representative);
(c) identification of the right that has allegedly been infringed;
(d) identification of the material or activity alleged to be unlawful;
(e) the URL, IP address, domain name or other location of the material;
(f) the remedial action requested;
(g) a statement that the complainant is acting in good faith; and
(h) a statement that the information in the notification is, to the complainant's knowledge, true and correct.

18.2 On receiving a complaint or notification, we may (as appropriate and lawful): forward it to the affected customer; request further information; remove, disable or block access to the content; suspend the affected service; preserve relevant information; refer the matter to law enforcement or a regulator; take no action where the notification is insufficient, abusive or not legally substantiated; or take any other action available under law or contract.

18.3 If we remove or disable content, this does not mean we accept liability for the content or make any finding on the merits of any dispute between the complainant and the customer. A person who lodges a notification wrongfully, or who makes a material misrepresentation, may be liable for resulting damages.

19. Reporting abuse

Abuse reports may be sent to legal@cipherwave.co.za and should include: your name and contact details; the IP address, domain, URL, email address, number or account involved; the date, time and time zone of the incident; supporting logs, headers or screenshots; a description of the abuse; and any urgent risk requiring immediate action. We may be unable to investigate complaints that lack sufficient technical detail.

20. Cooperation with law enforcement and regulators

20.1 We may cooperate with law-enforcement agencies, regulators, courts and other competent authorities where required or permitted by law, including by preserving data; providing subscriber, billing, usage or technical information; complying with lawful interception-related obligations; responding to warrants, subpoenas, court orders and regulatory notices; and taking steps to prevent or mitigate harm.

20.2 We may notify the customer of a request where lawfully permitted, but we are not obliged to do so where prohibited by law, court order, regulatory direction, operational necessity or security risk.

21. Our rights if this Policy is breached

21.1 If we reasonably believe this Policy has been breached, or that continued provision of the services may cause harm or expose us to risk, we may (proportionately to the breach): issue a warning; require remediation; require removal of content or disabling of a service; block, filter, rate-limit, quarantine or null-route traffic; suspend, restrict or disconnect the affected service; disable compromised credentials; remove or block access to unlawful or abusive content; recover reasonable costs incurred; report the matter to law enforcement, regulators, affected networks or industry bodies; terminate the agreement or affected service; refuse future service; and/or take legal action.

21.2 Where reasonably possible, and unless urgent action is required, we will give notice and a reasonable opportunity to remedy before suspending or terminating a service. We may act **without prior notice** only where: there is an emergency or material security risk; we are required to act by law, court order or competent authority; the service is being used for unlawful or seriously harmful activity; continued service may harm our network, customers or third parties; you cannot reasonably be reached;

prior notice may worsen the harm or prejudice an investigation; or the breach is serious, repeated or deliberate.

21.3 Where you are a consumer or subscriber protected by the Consumer Protection Act 68 of 2008 or the ICASA End-user and Subscriber Service Charter Regulations, 2016, we will exercise our rights under this clause in accordance with those protections, including applicable notice, complaints and redress requirements.

22. Suspension, termination and liability

22.1 Suspension or termination under this Policy does not limit any other right or remedy available to us. You remain liable for all charges incurred before suspension or termination, any applicable termination charges under your agreement, and recoverable costs caused by your breach (including remediation, investigation, blacklisting-removal, and legal and third-party costs).

22.2 To the extent permitted by law, we are not liable for loss of service, data, revenue, profits or goodwill resulting from a lawful suspension, restriction, removal, blocking or termination under this Policy. Nothing in this Policy excludes or limits any liability that cannot lawfully be excluded or limited, including under the Consumer Protection Act 68 of 2008.

23. Your indemnity

To the fullest extent permitted by law, you indemnify us, our officers, employees, contractors and upstream providers against claims, losses, liabilities, damages, penalties and reasonable costs arising from your breach of this Policy; unlawful or unauthorised use of the services; content you or your users host, transmit or make available; infringement of third-party rights; spam, cyber abuse, malware, phishing, fraud or network abuse involving your account or systems; compromise of your systems, credentials or PBX; your failure to comply with law; or claims by your users or third parties relating to your use of the services. This clause is subject to any protections you enjoy under the Consumer Protection Act 68 of 2008.

24. Data backups

Unless expressly agreed in writing, you are responsible for backing up your own data, content, configurations, email, databases, websites and applications. We are not responsible for loss, corruption or restoration of data except to the extent expressly agreed in a service-specific agreement or required by law.

25. Changes to this Policy

We may amend this Policy from time to time. We will publish the current version on our website with its version number and effective date, and will retain superseded versions. Where required by law, or where changes materially affect consumer customers, we will give reasonable advance notice of material changes. Continued use of the services after the effective date constitutes acceptance of the amended Policy, subject to your rights under applicable law and your agreement.

26. Order of precedence

If there is a conflict between this Policy and another applicable document, the following order applies unless stated otherwise: (1) a signed written agreement with you; (2) product-specific terms; (3) the service level agreement; (4) the fair usage policy; (5) this Acceptable Use Policy; (6) website terms. However, nothing in any document permits unlawful or abusive use of the services.

27. Complaints and dispute resolution

If you believe we have incorrectly applied this Policy, you may complain to legal@cipherwave.co.za or in writing to Attention the CEO at CipherWave Address: Building 7, Waterfall Office Park, 74 Waterfall

Drive, Waterfall City, Midrand ,1684. Your complaint should include your account number, contact details, the affected service, relevant dates and a description of the issue. We will handle complaints in accordance with our complaints procedure and applicable regulatory requirements, including (where applicable) the ICASA End-user and Subscriber Service Charter Regulations, 2016. Where those Regulations apply, unresolved complaints may be escalated to ICASA or to alternative dispute resolution as provided for in those Regulations.

28. Contact details

Abuse reports: Abuse@cipherwave.co.za
Take-down notices: legal@cipherwave.co.za
Customer support: support@cipherwave.co.za
Privacy queries / Information Officer: info@cipherwave.co.za
Website: www.cipherwave.co.za
Registered address: Building 7, Waterfall Office Park, 74 Waterfall Drive, Waterfall City, Midrand ,1684

This Acceptable Use Policy forms part of the terms governing the use of CipherWave's services. Customers are responsible for ensuring that all users of their services comply with it.