ACCEPTABLE USE POLICY

COMNEXIA Corporation

Website-Hosted Customer Policy

Version 2026.08.14

Intended permanent URL

https://comnexia.com/acceptable-use-policy/

How this policy applies. This AUP applies only when a Customer Sales Order expressly incorporates it. It supplements, and does not replace, the Master Services Agreement (MSA). If this AUP conflicts with a document higher in the MSA order of precedence, the higher document controls.

COMNEXIA Corporation
590 W Crossville Road, Suite 201
Roswell, Georgia 30075
(877) 600-6550 | info@comnexia.com

1. Purpose and Scope

This Acceptable Use Policy ("AUP") protects COMNEXIA, its Customers, Third-Party Providers, networks, systems, personnel and the public from unlawful, abusive, unsafe or disruptive use of Services.

Customer is responsible for compliance with this AUP by its employees, contractors, users and other persons who access or use Services through Customer accounts, systems or credentials.

2. Prohibited Illegal or Harmful Activity

Customer may not use Services to violate applicable law, facilitate unlawful conduct, or knowingly cause material harm to another person, system, network or service.

- Fraud, identity theft, deceptive schemes, extortion, unlawful gambling, unlawful trafficking, or other criminal activity.
- Threats, stalking, harassment, exploitation, or distribution of unlawful content.
- Material infringement or misappropriation of copyright, trademark, patent, trade secret, privacy, publicity or other protected rights.
- Use prohibited by applicable export-control, sanctions or trade laws.

3. Unauthorized Access and Security Abuse

- Accessing or attempting to access an account, device, application, network, data set or system without authorization.
- Probing, scanning, penetration testing, password spraying, credential stuffing, vulnerability exploitation or similar activity without the system owner's express authorization and any required COMNEXIA approval.
- Bypassing authentication, access controls, rate limits, endpoint security, monitoring, filtering, logging or other security controls.
- Introducing, distributing, executing or facilitating malware, ransomware, spyware, botnets, malicious scripts or destructive code.
- Using compromised credentials or knowingly allowing unauthorized persons to use Customer credentials.

4. Email, Messaging and Communications Abuse

- Sending spam, unsolicited bulk messages or commercial communications in violation of applicable law or Third-Party Provider rules.
- Phishing, impersonation, spoofing, business email compromise, credential harvesting or deceptive sender identification.
- Using purchased, scraped or harvested contact lists in a manner that violates law, consent requirements or provider rules.
- Continuing to send communications after a recipient has validly opted out where an opt-out right applies.
- Operating a mail or messaging system in a manner that materially damages COMNEXIA or Third-Party Provider reputation, deliverability or network standing.

5. Network and Resource Abuse

- Denial-of-service attacks, flooding, intentional overload, broadcast abuse or other conduct intended to impair availability.
- Excessive or abnormal consumption that materially interferes with shared infrastructure, unless the applicable Service expressly permits that level of use.

- Operating open relays, open proxies, anonymization infrastructure or externally accessible services that create a material abuse or security risk without appropriate safeguards.
- Using IP addresses, domains, telephone numbers, licenses or other resources assigned by COMNEXIA outside the authorized Service scope.

6. Privacy, Data and Content

Customer must have the legal rights and permissions necessary for data and content it stores, transmits, processes or directs COMNEXIA to process. Customer may not use Services to unlawfully collect, disclose, sell, intercept, monitor or process personal, confidential or regulated information.

7. Security Testing

Customer must not test COMNEXIA systems, shared infrastructure or another customer environment without COMNEXIA's prior written authorization. Testing of Customer-owned systems may also require coordination when it could affect COMNEXIA-managed infrastructure, monitoring, Third-Party Providers or other customers.

8. Third-Party Provider Rules

Customer must comply with acceptable-use, licensing, security, messaging, telecommunications and other use restrictions imposed by Third-Party Providers for products Customer receives through COMNEXIA. A Third-Party Provider may independently suspend or restrict a product when its rules are violated.

9. Investigations and Protective Measures

COMNEXIA may reasonably investigate suspected abuse, security threats or violations. Customer will cooperate with reasonable requests for information necessary to investigate or contain a problem.

COMNEXIA may block traffic, disable credentials, isolate a device, suspend an affected Service or take other reasonable protective action when permitted by the MSA and reasonably necessary to address unlawful activity, abuse, an active security threat or material risk.

10. Remediation Costs

If Customer causes a material AUP violation, Customer is responsible for reasonable remediation work, provider charges, equipment costs and other direct costs COMNEXIA incurs to investigate, contain or correct the violation, at the rates otherwise applicable under the Agreement. This section does not create a fixed incident fee.

11. No Service Credits for Customer-Caused Interruption

Unless an applicable SLA expressly states otherwise, Customer is not entitled to a service credit for an interruption caused by Customer's violation of this AUP, Customer-directed suspension, unlawful use, compromised Customer credentials or reasonable protective action required because of Customer activity.

12. Changes to this AUP

COMNEXIA may update this AUP in the manner permitted by the MSA to address changes in law, security threats, abuse patterns, Third-Party Provider requirements or reasonable industry practices. The version applicable to Customer is determined under the MSA and applicable Sales Order.

13. Reporting Abuse

Reports concerning suspected abuse of COMNEXIA Services may be sent to abuse@comnexia.com. Security emergencies should also be reported through COMNEXIA's normal support or emergency-support channels.