RENVOZ

Acceptable Use & Responsible Access Policy

---

1. Introduction

This Acceptable Use & Responsible Access Policy (“Policy”) defines the rules, obligations, and standards for the proper use of RENVOZ platforms, communication systems, applications, digital services, and network infrastructure.

The objectives of this Policy are to:

- Encourage secure, lawful, and ethical use of RENVOZ resources
- Protect company systems, customer information, and operational continuity
- Maintain the integrity, reliability, and performance of RENVOZ services
- Ensure compliance with applicable legal, regulatory, and industry requirements
- Reduce risks associated with misuse, unauthorized access, and cyber threats

---

2. Applicability

This Policy applies to every individual or organization that accesses, connects to, manages, or uses RENVOZ systems or services, including:

- Employees and staff members
- Customers and subscribers
- Contractors, consultants, and temporary workers
- Vendors, suppliers, and integration partners
- Third-party service providers and affiliates

Use of RENVOZ services constitutes acceptance of this Policy and all associated requirements.

---

3. Principles of Acceptable Use

Users are expected to act responsibly and use RENVOZ resources only for authorized and legitimate purposes.

3.1 Authorized Operations

RENVOZ systems and services must be used solely for approved business, communication, operational, or customer-related activities.

3.2 Compliance Obligations

Users must comply with all applicable laws, telecommunications regulations, privacy standards, intellectual property rights, and contractual obligations.

3.3 Ethical Usage

Users must avoid any conduct that may compromise the confidentiality, availability, security, or reputation of RENVOZ or its clients.

---

4. Restricted and Prohibited Conduct

The activities listed below are strictly forbidden while using RENVOZ infrastructure or services.

4.1 Unlawful Activities

Users may not use RENVOZ systems for illegal purposes, including fraud, unauthorized surveillance, identity theft, or violations of communication laws and regulations.

4.2 Unauthorized Access or Security Abuse

Users are prohibited from attempting to:

- Access systems, accounts, or data without authorization
- Circumvent authentication or security protections
- Introduce malicious software, ransomware, spyware, or harmful code
- Exploit vulnerabilities or perform security testing without written approval
- Interfere with monitoring, logging, or audit mechanisms

4.3 Service Disruption or Network Misuse

Activities intended to interrupt, overload, or degrade services are prohibited, including:

- Distributed denial-of-service (DDoS) attacks
- Excessive bandwidth consumption
- Automated traffic flooding
- Network interference or service manipulation

4.4 Unsolicited Communications

Users may not distribute:

- Spam or bulk unsolicited messages
- Unauthorized robocalls or automated communications
- Fraudulent marketing campaigns or deceptive promotions

4.5 Misrepresentation or Deception

Users must not impersonate any person, organization, or entity, nor falsify caller identification, authentication credentials, routing data, or account information.

4.6 Harmful or Inappropriate Content

RENVOZ services must not be used to transmit or distribute material that is:

- Threatening or abusive
- Defamatory or harassing
- Discriminatory or hateful
- Obscene, fraudulent, or otherwise unlawful

4.7 Attempts to Evade Security Controls

Any effort to bypass access restrictions, encryption safeguards, security tools, or monitoring systems is prohibited.

---

5. User Duties and Security Responsibilities

All users are expected to:

- Protect confidential, sensitive, and proprietary information
- Maintain the confidentiality of passwords and authentication credentials
- Use company systems professionally and responsibly
- Promptly report suspicious activity, security weaknesses, or policy violations
- Cooperate with security investigations when required
- Follow all contractual, legal, and compliance obligations applicable to their role or services

Failure to meet these responsibilities may result in disciplinary or legal action.

---

6. Monitoring, Logging & Privacy

RENVOZ may monitor, inspect, record, or audit the use of its systems, applications, communications, and network resources for purposes including:

- Security monitoring
- Threat detection and prevention
- Regulatory compliance
- Service performance and operational integrity
- Investigation of suspected misuse or unauthorized activity

All monitoring activities will be conducted in accordance with applicable privacy and data protection laws.

---

7. Violations and Enforcement Measures

RENVOZ reserves the right to take appropriate action in response to violations of this Policy. Actions may include:

- Suspension of accounts or services
- Permanent termination of access privileges
- Blocking or removal of unauthorized activity or content
- Administrative or disciplinary measures
- Financial recovery for damages or losses caused
- Referral to law enforcement or regulatory authorities where applicable

RENVOZ retains sole discretion in determining the appropriate response to any violation.

---

8. Reporting Security Incidents or Policy Violations

Any suspected misuse, policy violation, cybersecurity issue, or unauthorized activity must be reported immediately to:

RENVOZ Compliance & Security Team
Email: compliance@renvoz.com

---

9. Acknowledgment and Acceptance

By accessing, using, or interacting with RENVOZ systems, services, platforms, or infrastructure, users confirm that they:

- Have read and understood this Policy
- Agree to comply with all requirements outlined herein
- Accept responsibility for activities conducted under their access credentials

10. Updates and Policy Modifications

RENVOZ reserves the right to revise, amend, or replace this Policy at any time to reflect operational, legal, security, or regulatory changes.

Revised versions become effective immediately upon publication or official distribution.

RENVOZ

Acceptable Use & Responsible Access Policy