

# Acceptable Use Policy (AUP)

## 1. Purpose

This Acceptable Use Policy (AUP) outlines the standards and expectations for the appropriate, ethical, and lawful use of Renvyo's technology resources, services, and network infrastructure. The objective of this policy is to promote responsible use, ensure compliance with applicable laws and regulations, and protect the integrity, security, and reputation of the organization.

## 2. Scope

This policy applies to all individuals who access or use Renvyo's systems, services, or network infrastructure. This includes employees, contractors, clients, business partners, vendors, and any third parties who are granted authorized access to company resources.

## 3. Acceptable Use Guidelines

All users are expected to utilize Renvyo's technology resources responsibly and in accordance with the following guidelines:

- **Business-Related Use:** Company resources should primarily be used for legitimate business activities that support the organization's operations and objectives.
- **Legal Compliance:** All activities conducted through Renvyo's systems must comply with applicable local, national, and international laws and regulations.

## 4. Prohibited Activities

The following activities are strictly prohibited when using Renvyo's systems or network infrastructure:

- Engaging in any form of illegal activity

- Attempting to breach or compromise system or network security
- Interfering with network operations, performance, or service availability
- Sending unsolicited communications such as spam
- Misrepresenting identity or impersonating another individual or organization
- Accessing, distributing, or transmitting offensive, harmful, or inappropriate content
- Circumventing or attempting to bypass established security controls or safeguards

## **5. User Responsibilities**

Users are responsible for protecting the security and integrity of Renvyo's systems and data. This includes safeguarding sensitive information, following established security procedures, and ensuring that their actions do not compromise the confidentiality, availability, or reliability of company resources.

## **6. Monitoring and Privacy**

Renvyo reserves the right to monitor the use of its systems and network infrastructure to ensure compliance with this policy, maintain operational security, and protect organizational assets. Any monitoring activities will be conducted in accordance with applicable privacy laws and regulations.

## **7. Enforcement and Consequences**

Violations of this Acceptable Use Policy may result in disciplinary actions, including suspension of access privileges, termination of services or employment, and, where applicable, legal action.

## **8. Reporting Incidents**

Any suspected violation of this policy or any security-related concern should be reported immediately to the Compliance Officer at: [compliance@renvyo.com](mailto:compliance@renvyo.com)

## **9. User Agreement**

By accessing or using Renvyo's systems, services, or network infrastructure, users acknowledge that they have read, understood, and agree to comply with the terms of this Acceptable Use Policy.

## **10. Policy Revisions**

Renvyo reserves the right to modify or update this Acceptable Use Policy at any time. Users are encouraged to review this policy periodically to stay informed about any updates or changes.