

ACCEPTABLE USE POLICY (AUP)

1. Purpose

This Acceptable Use Policy (“AUP”) establishes the standards, expectations, and responsibilities governing the appropriate and lawful use of NETVOICELINK’s technology resources, services, systems, and network infrastructure.

The purpose of this policy is to:

- Promote ethical, secure, and responsible use of company resources
- Ensure compliance with applicable laws and regulations
- Protect the confidentiality, integrity, and availability of systems and data
- Safeguard the reputation and operational reliability of NETVOICELINK

2. Scope

This policy applies to all individuals and entities who access, use, or interact with NETVOICELINK’s services or infrastructure, including but not limited to:

- Employees
- Contractors and consultants
- Customers and clients
- Vendors and partners
- Third-party users and affiliates

By accessing or using NETVOICELINK services, users agree to comply with this AUP.

3. Acceptable Use Guidelines

Users are expected to utilize NETVOICELINK resources in a professional, ethical, and lawful manner.

3.1 Authorized Business Use

NETVOICELINK services and systems are intended primarily for legitimate business and operational purposes.

3.2 Legal and Regulatory Compliance

All users must comply with applicable local, national, and international laws, regulations, and industry standards while using NETVOICELINK services.

3.3 Responsible Conduct

Users must conduct themselves in a manner that does not compromise the security, performance, or reputation of NETVOICELINK or its customers.

4. Prohibited Activities

The following activities are strictly prohibited:

4.1 Illegal Activities

Using NETVOICELINK services for any unlawful purpose, including fraud, unauthorized access, or violations of telecommunications regulations.

4.2 Security Violations

Attempting to:

- Gain unauthorized access to systems or networks
- Interfere with security mechanisms
- Distribute malware, viruses, or malicious code
- Exploit vulnerabilities or conduct penetration attempts without authorization

4.3 Network Abuse

Activities that disrupt or negatively impact network operations, including:

- Excessive traffic generation
- Denial-of-service attacks
- Network interference or service degradation

4.4 Spam and Unsolicited Communications

Sending unsolicited bulk communications, spam, robocalls, or unauthorized marketing messages.

4.5 Identity Misrepresentation

Impersonating another person, entity, or organization, or falsifying caller identification or authentication information.

4.6 Offensive or Harmful Content

Transmission or distribution of content that is abusive, defamatory, discriminatory, threatening, or otherwise inappropriate.

4.7 Circumvention of Security Controls

Attempting to bypass authentication systems, access restrictions, monitoring tools, or security safeguards.

5. User Responsibilities

Users are responsible for:

- Protecting confidential and sensitive information
- Maintaining the security of account credentials and authentication data
- Using systems responsibly and professionally
- Promptly reporting suspected security incidents or unauthorized activity
- Complying with all applicable regulatory and contractual obligations

Failure to fulfill these responsibilities may result in corrective action.

6. Monitoring and Privacy

NETVOICELINK reserves the right to monitor, review, and audit the use of its systems, services, and network infrastructure to ensure compliance with this policy, maintain operational integrity, and protect against unauthorized activities.

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

7. Enforcement and Consequences

Violations of this AUP may result in one or more of the following actions:

- Temporary or permanent suspension of services
- Restriction or termination of access privileges
- Removal of unauthorized content or activity

- Legal action or referral to law enforcement authorities
- Financial liability for damages caused by policy violations

NETVOICELINK reserves the right to take appropriate action at its sole discretion.

8. Reporting Violations or Security Incidents

Any suspected violation of this policy or security-related incident should be reported immediately to:

Compliance Officer

Email: compliance@netvoicelink.com

9. User Agreement

By accessing or using NETVOICELINK services, systems, or infrastructure, users acknowledge that they have read, understood, and agreed to comply with this Acceptable Use Policy.

10. Policy Revisions

NETVOICELINK reserves the right to modify or update this Acceptable Use Policy at any time without prior notice.

Updated versions of the policy will become effective upon publication.

NETVOICELINK
Acceptable Use Policy (AUP)
© All Rights Reserved.