

Acceptable Use Policy (AUP)

This Acceptable Use Policy (“Policy” or “AUP”) is established to ensure the safe, lawful, stable, and uninterrupted use of all services provided by Atak Domain Bilgi Teknolojileri A.Ş. (“Atak Domain”, “We”).

All customers (“Customer”), resellers (“Reseller”), end users, and any parties offering Atak Domain services to third parties agree to comply with this Policy.

This Policy applies to all services provided by Atak Domain, including but not limited to domain name services, hosting, DNS services, email services, SSL certificates, cloud services, API services, forwarding services, proxy/privacy services, and any related offerings.

1. Purpose and Scope

The purpose of this Policy is to:

- Ensure the safe, lawful, and good-faith use of Atak Domain services
- Prevent misuse, illegal use, and harmful activities
- Protect third parties, internet users, and system infrastructure from damage
- Maintain compliance with ICANN, IANA, registry operators, and all relevant global regulatory frameworks

This Policy applies to individual Customers, Resellers, and their end users.

1

2. Prohibited Activities

Atak Domain services may **not** be used for any of the following purposes.

2.1 Illegal Activities

The following actions are strictly prohibited:

- Fraud, scam, phishing
- Money laundering or financial fraud
- Illegal gambling, betting, unauthorized payment systems
- Unauthorized sale of drugs, weapons, medical devices
- Copyright infringement, distribution of pirated content
- Deepfake or identity fraud
- Hate speech, violence, terrorist propaganda
- Unauthorized sharing of personal data
- Violations of national or international sanctions
- Human trafficking, exploitation, threats

Atak Domain may immediately suspend services upon detection of illegal activity.

3. DNS Abuse

DNS abuse includes the following harmful activities as defined by ICANN:

- Phishing
- Malware or ransomware distribution
- Botnet or command-and-control (C2) operations
- Pharming and DNS manipulation
- Fast-Flux hosting
- Using spam as a malware distribution method
- Participating in or organizing DDoS attacks

Atak Domain may suspend a domain or service without prior notice if DNS abuse is detected.

4. Hosting Abuse

Hosting services may not be used for:

- Cryptocurrency mining
- Torrent tracker, warez, or P2P nodes
- Resource-intensive bots or scripts
- Vulnerability scanners or brute-force tools
- Attack simulation or exploit distribution
- Unauthorized streaming of movies/TV (DMCA violations)
- Adult content that violates legal requirements
- Illegal APIs, proxy services, or VPN operations
- Spam creation or distribution

2

Atak Domain reserves the right to restrict, suspend, or terminate such services.

5. Email Abuse

The following email activities are prohibited:

- Bulk or unsolicited email (spam)
- Use of stolen or purchased email lists
- Email spoofing
- Sending harmful or malicious content
- Causing IP addresses to be blacklisted

If spam is detected, email services may be disabled.

6. Content Abuse

Atak Domain services may not be used to host or distribute:

- Child sexual abuse material (CSAM)
- Threats, violence, hate speech, harassment
- Copyright-infringing content
- Illegal products or services

- Fraudulent or deceptive content, identity impersonation
- Unauthorized data harvesting or scraping

Such content results in immediate service termination.

7. System and Network Security Abuse

The following behaviors are strictly prohibited:

- Unauthorized access (hacking)
- Port scanning, brute-force attacks
- MITM (Man-in-the-Middle) attacks
- Hosting malware
- Firewall evasion attempts
- Overloading servers
- Launching DoS/DDoS attacks

Atak Domain may immediately suspend affected services.

8. Resource Usage Policy

The following excessive resource usage behaviors are prohibited:

- Excessive CPU or RAM usage
- Large numbers of background processes
- Heavy cron jobs
- Excessive disk I/O usage
- High-volume or abusive database queries
- Any usage inconsistent with shared/limited hosting environments

Atak Domain may limit resources or suspend the service if misuse occurs.

9. Account Security and Customer Responsibilities

Customers are responsible for:

- Using strong passwords
- Keeping login credentials confidential
- Maintaining an up-to-date email address
- Keeping CMS/software updated
- Patching security vulnerabilities
- Preventing unauthorized access to their accounts

The Customer bears all responsibility for unauthorized use.

10. Reseller Responsibilities

Resellers must:

- Ensure that their end users comply with the AUP

- Respond quickly to abuse reports
- Prevent fraudulent registrations
- Detect forged or invalid documents
- Comply with KYC/AML requirements

Resellers may be held responsible for their customers' violations.

11. Abuse Reports

Notifications from the following sources are treated as high priority:

- ICANN / IANA
- Registry operators
- CERT / GovCERT teams
- Law enforcement
- CleanDNS, Spamhaus, APWG
- Banks and financial institutions

Atak Domain may take action without notifying the customer when required.

12. Enforcement Actions

In the event of a violation, Atak Domain may apply any of the following measures:

- Request removal of harmful content
- Suspend web hosting
- Suspend or lock the domain name
- Disable DNS records
- Terminate API access
- Close the account
- Report the issue to relevant authorities

The Customer accepts all legal and financial responsibility for violations.

13. Policy Amendments

Atak Domain reserves the right to modify or update this Policy at any time.

Updates become effective once published on the website.

14. Contact Information

For abuse notifications:

domain@apiname.com, hukuk@atakdomain.com

Address:

Atak Domain Bilgi Teknolojileri A.Ş.

İstasyon Mah. Efe Sadık Cad. No:4 İç Kapı No:2

Kartepe / Kocaeli – Türkiye

Phone: +90 262 325 9222