ATAK® Domain & Hosting ICANN

ABUSE PREVENTION POLICY

Atak Domain Bilgi Teknolojileri A.Ş. (“Atak Domain”, “We”, “Service Provider”) aims to maintain a safe, stable, and abuse-free internet ecosystem across all services it provides. This Abuse Prevention Policy (“Policy”) applies to all services offered by Atak Domain, including domain name registration, DNS, hosting, email, SSL, forwarding, proxy/protection services, and all other related services (collectively “Services”).

This Policy has been prepared in accordance with ICANN, IANA, TRABIS, RFC 2350, GDPR, eIDAS, the DNS Abuse Framework, Registrar Accreditation Agreement (RAA 3.18), and global industry standards. The latest version of this Policy is published on Atak Domain’s website and becomes effective immediately upon publication.

1. PURPOSE OF THE POLICY

This Policy has two primary objectives:

1.1 Ensuring user and public safety

Atak Domain supports efforts to protect internet users from harmful activities such as:

- fraud
- phishing
- malware
- botnet activity
- data theft
- trademark abuse
- child sexual abuse material (CSAM)

1.2 Guiding the reporting and intervention process

This Policy informs customers about what constitutes abuse and how such cases may be reported to Atak Domain.

2. SCOPE OF THE POLICY

The following services are fully subject to this Policy:

- Domain name registration & transfer
- DNS & Nameserver services
- Hosting (shared, cloud, VPS, WordPress, reseller)
- Email services
- SSL and security products
- Domain proxy/ID protection
- Forwarding / redirection
- All API-based services

All users and resellers using Atak Domain Services are deemed to have accepted this Policy explicitly and implicitly.

3. ATAK DOMAIN'S INTERVENTION AUTHORITY

In line with global standards and at its sole discretion, Atak Domain may take the following actions:

- Suspend the service
- Disable DNS
- Lock the domain
- Reveal WHOIS data / remove privacy protection
- Disable hosting content
- Terminate API access
- Apply transfer lock
- Disable or block content
- Comply with court orders
- Respond to law enforcement requests

This authority is based on RAA 3.18.1, the DNS Abuse Framework, and international regulations.
Atak Domain may take immediate action *without prior notice* in cases involving malicious or clearly unlawful activity.

4. TYPES OF ABUSE

The classification below follows global standards.

4.1 DNS Abuse (per ICANN & DNS Abuse Framework)

a) **Malware distribution**
Viruses, trojans, ransomware, keyloggers, etc.

b) **Botnet & Command-and-Control (C2)**
Botnet management, propagation mechanisms.

c) **Phishing**
Impersonation of legitimate entities to steal data.

d) **Pharming / DNS Manipulation**
DNS poisoning, hijacking, fast-flux hosting.

e) **Spam (when used as a vector for DNS Abuse)**
Spam alone is not DNS Abuse; only when used to deliver malware, phishing, or fraud.

4.2 Content Abuse (Hosting Abuse)

a) **Intellectual property violations** (DMCA / copyright / trademark abuse)
b) **Child sexual abuse material (CSAM)**
Absolutely prohibited. Immediate takedown → law enforcement notification.
c) **Hate speech & terrorist content**
d) **Personal data violations (Doxxing)**
e) **Illegal product or service sales**
f) **Human trafficking / exploitation content**

4.3 Other Illegal Uses

- Fraud / scam
- Fake technical support scams
- Crypto investment scams
- Recovery scams
- Fake payment services
- Copyrighted content distribution
- Impersonation
- Violations of sanctions (OFAC, EU sanctions)
- Hacking activities
- Hosting DDoS tools

5. RESTRICTED USE (Requires compliance with regulations)

The following categories are not entirely prohibited but must comply with relevant regulations:

- Adult content (age verification required)
- P2P / torrent / file-sharing infrastructure
- IRC/chat hosting
- Streaming & download hosting
- Bulk email (must comply with data protection and opt-in requirements)

6. TRUSTED NOTIFIERS

Atak Domain considers the following as “Trusted Notifiers,” similar to global best practices:

- National / international law enforcement agencies
- CERT / CSIRT teams
- ICANN DAAR reports
- Recognized anti-abuse organizations
- Official brand representatives
- Registry operators (Verisign, PIR, Identity Digital, GMO, NIC.TR)
- INTERPOL / EUROPOL cybercrime units

Reports from these entities receive immediate priority.

7. HOW TO REPORT ABUSE

Abuse Email Addresses:
domain@apiname.com, hukuk@atakdomain.com

Reports should include:

- Full URL where the violation was detected
- Supporting evidence
- Email headers (for email-related abuse)
- Screenshots
- Log or traffic data
- Brief description of the observed behavior
- Reporter’s contact information
- If geographically/device-restricted, details (e.g., “visible only from US IPs”)

Multiple incidents → must be consolidated in a single report.
Anonymous, incomplete, or unsupported reports may not be processed.

8. REPORT REVIEW AND RESPONSE PROCESS

Atak Domain follows Global Abuse Standards.

8.1 Initial Review (0–24 hours)

Report received → ticket assigned → category identified → customer may be notified.

8.2 Verification (0–48 hours)

Evidence is reviewed. Abuse cannot be confirmed if inaccessible or unsupported.

8.3 Intervention (Emergency / Low Risk)

- CSAM / malware / phishing → Immediate suspension
- Botnet / C2 → Action within 6 hours
- Trademark / DMCA → Within 2 business days
- Hosting content violation → 1–3 business days
- WHOIS inaccuracy → 7 days allowed for correction

8.4 Feedback

In some cases, specific actions cannot be disclosed due to legal constraints.

9. CUSTOMER RESPONSIBILITIES

- Not using Services unlawfully
- Keeping WHOIS information accurate

- Ensuring hosting and email security
- Responding to abuse notifications promptly
- Configuring API and panel integrations securely

10. VIOLATIONS AND ENFORCEMENT

The following actions may be applied:

- Suspension of Services
- Disabling content
- Domain locking
- Disclosure of WHOIS information
- Account termination
- Contract termination
- Reporting to law enforcement

Atak Domain may take action without prior notice when necessary to prevent harm.

11. GOVERNING LAW

- Turkish law applies.
- Jurisdiction: Kocaeli Courts.
- In international matters, relevant foreign laws may also be considered.