Email Usage Fair Limit Policy

1. General Provisions

This Email Usage and Fair Use Policy (“Policy”) is implemented to ensure the secure, stable, and uninterrupted operation of all email services provided by Atak Domain.

This policy applies to:
- shared hosting email services
- corporate email services
- webmail services
- SMTP, IMAP, POP3 access
- API-based email sending
- all email infrastructures not intended for bulk email sending

Every customer is deemed to have accepted this policy prior to using the service.

2. Purpose and Scope

The purpose of this Policy is to:

1. prevent misuse of the email infrastructure,
2. block spam, phishing, malware, and malicious sending activities,
3. protect server performance,
4. prevent email service disruptions affecting other customers.

This Policy covers all forms of email sending, receiving, storage, and processing.

3. Email Sending Limits (Fair Use Limits)

Atak Domain applies email sending limits in line with global standards.

3.1 SMTP Sending Limits

Package Type	Hourly Limit	Daily Limit
Shared Hosting	90 emails	500 emails
Corporate Email	200 emails	1000 emails
Dedicated Server/VPS	dependent on configuration	dependent on configuration

3.2 Webmail Limits

destek@atakdomain.com
atakdomain.com
İstasyon Mahallesi Efe Sadık Caddesi No: 4 İç Kapı No: 2 Kartepe, Kocaeli, TR

- Maximum 20 sends per minute
- Up to 15 simultaneous connections
- Maximum attachment size: 15 MB

4. Prohibited Email Usage

The following behaviors are strictly prohibited:

4.1 Spam Sending

- sending to lists without opt-in consent
- using purchased email lists
- newsletter sending without an unsubscribe link
- using the infrastructure as a spam distribution system

4.2 Sending Harmful Content

- trojans, malware, ransomware
- phishing pages or deceptive clone sites
- misleading or fraudulent links
- illegal content

4.3 Service Overload

- overloading IMAP/POP3 with excessive synchronization
- opening hundreds of simultaneous IP connections
- excessive API/control panel queries via scripts

4.4 Malicious Use

- brute-force attacks
- attempts to open unauthorized SMTP relay
- sending emails via botnets

5. Violation Detection and Actions Taken

Atak Domain may detect misuse through the following methods:

- SMTP log analysis
- real-time sending volume analysis
- spam blackhole / RBL list monitoring
- complaint reports
- security scans
- AI-based spam behavior detection

In case of violation, the following actions may be taken:

5.1 Level 1 – Warning

• Customer is notified
• Sending may be limited until the issue is resolved

5.2 Level 2 – Account Suspension

• Email sending is halted
• Receiving may also be temporarily disabled if necessary

5.3 Level 3 – Permanent Ban / IP Block

• IP address may be permanently blocked
• Account may be terminated
• Information may be shared with affected third-party organizations
• Legal action may be taken if required

6. Blacklist Policy

If the SMTP or IP address appears on blacklists such as:
• Spamhaus
• UCE Protect
• CBL
• Barracuda
• Microsoft SNDS
• Gmail Postmaster

then:
• a cleanup process is initiated,
• IP change may be applied if necessary,
• the customer is notified promptly.

If the customer repeatedly causes blacklisting:
• the service may be suspended,
• the contract may be terminated,
• the customer may be held responsible for all associated costs.

7. Cold Email Policy

Cold emailing is prohibited on shared hosting and standard email infrastructures. Cold email = sending commercial messages to recipients with whom no prior relationship exists.

For such mailings, the customer must use:
• a dedicated server
• a dedicated IP
• a bulk mailing infrastructure

8. Mailbox Storage Limits

Storage limits:
• Shared hosting: 250 MB per mailbox
• Corporate email: 5–100 GB per mailbox
• Additional storage may be added via package upgrades

Exceeding storage limits may:
• block new incoming mail,
• cause inbox overflow,
• reduce performance.

10. Customer Responsibilities

The Customer is responsible for:
• protecting email passwords,
• not sharing access credentials with third parties,
• avoiding login from infected devices,
• regularly updating mailing lists,
• cooperating with Atak Domain in case of spam complaints.

Atak Domain is not responsible for deliverability issues arising from incorrect customer configurations.

11. Data Security and Privacy

Atak Domain:
• does not read email contents,
• fully adheres to privacy principles,
• complies with KVKK & GDPR regulations,
• securely stores logs.

12. Policy Updates

This Policy may be updated by Atak Domain due to technical requirements, global anti-spam standards, or legal regulations.
Updates become effective immediately upon publication on the website.

destek@atakdomain.com
atakdomain.com
İstasyon Mahallesi Efe Sadık Caddesi No: 4 İç Kapı No: 2 Kartepe, Kocaeli, TR