Two-Factor Authentication (2FA) Terms of Use

1. **Introduction**
   Two-Factor Authentication ("2FA") allows two different methods to be used together for identity verification in order to enhance the security of access to your account. You have the option to enable the 2FA feature for your account. When you enable 2FA, you are deemed to have accepted these Two-Factor Authentication Terms of Use ("2FA Terms of Use") and you declare and undertake that you prefer to use a login process that is different from, and more secure than, the standard Control Panel login process.

These 2FA Terms of Use come into force as of the date on which 2FA is enabled on your account, between:

Domain Name API – the brand under which services are provided via www.domainnameapi.com
Atakonline Domain Hosting İnternet ve Bilgi Teknolojileri LTD ("we", the Service Provider)

and the person or entity enabling 2FA ("you", the User).

The terms "you" and "your" in this text refer to the natural or legal person who enables 2FA on their account. These 2FA Terms of Use do not create any right or benefit in favour of any third party.

2. **Enabling 2FA**
   To enable 2FA for your account, you must download an approved Two-Factor Authentication (2FA) / One-Time Password (OTP) application to your smartphone and link this application to your account on the Domain Name API Control Panel.

In this context:

- After logging in to the Control Panel,
- You can follow the relevant menu steps (if you are using the new DNA panel, via the menu at the top right such as *My Account* > *Two-Factor Authentication (2FA)*, etc. – 2FA is mandatory for new resellers; if you are using the existing DNA panel, via the left menu such as *My API Settings* > *Two-Factor Authentication*, etc.),
- And by following the on-screen instructions, you pair your smartphone application with your account.

Once the 2FA application has been linked to your account, access to your account will require, in addition to your standard username and password, the entry of the one-time verification code periodically generated by the smartphone application.

3. **Login (Sign-in) Process**
   After you enable 2FA for your account, the authentication information you must use to access your account changes and the login process becomes two-step.

In this new login process:

1. You enter your username and password, and
2. You then enter the security code generated by the 2FA/OTP application on your smartphone.

Once 2FA is enabled, the standard single-step login method consisting only of username and password is disabled, and it is no longer possible to access your account using that method. By enabling 2FA, you accept this new two-step login process.

4. **Copying and Storing the QR Code / Text Code**
   When you enable 2FA for the first time via the Control Panel, a QR code and/or text code specific to your account is displayed on the screen.

You accept and undertake that:

- You will make a secure copy of this page (for example, by taking a screenshot or making a secure note), and
- You will store this copy in a secure location to which no third party has access.

This backup QR/text code is required so that you can regain access to your account in situations such as:

- Losing your smartphone,
- Losing access to your device,
- Deletion or corruption of the application,
- Becoming unable to generate 2FA codes.

Losing this code may make the recovery of your account difficult or cause delays.

5. **Manual Recovery**
   You accept that you are responsible for securely storing the backup QR code / text code.

You further accept that:

- If you lose this backup code and become unable to generate 2FA codes, and
- Therefore request manual intervention for the recovery of your account,

the Service Provider may be required to perform additional steps to verify your identity and account ownership, and in this context reserves the right to charge a reasonable service fee.

Since the manual recovery process may require additional security checks, document requests and technical review:

- The duration of the recovery process cannot be guaranteed in advance, and
- You accept that access to your account may be temporarily unavailable during this period.

6. **Accuracy of Your Account Information**
   During the manual recovery process, you will be contacted based on the contact information registered on your account. In this context, you declare and undertake that:

- The fax number registered on your account (if any),
- Your telephone number,
- Your postal code and, where deemed necessary, your other contact details

are accurate and up to date.

This information will be used for identity and account verification in the event of a manual recovery request. You accept that you are obligated to promptly update the information registered on your account in case of any change.

7. **Third-Party One-Time Password (OTP) Applications**
   The third-party One-Time Password (OTP) application (such as Google Authenticator, Authy, etc.) that you will use on your smartphone (or tablet) for 2FA is entirely subject to the terms and conditions of the respective application provider.

In this context, you accept that:

- The use, updates, security, performance and continuity of the third-party OTP application are solely subject to the relationship between you and the relevant application provider.
- The Service Provider is not liable for any:
    - performance issue,
    - data loss,
    - security vulnerability,
    - breach, incompatibility or damage

arising from or related to this third-party application. You accept that you assume these risks yourself by installing and using the relevant OTP application.

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