Data Breach Response Policy

Atak Domain Bilgi Teknolojileri A.Ş.

1. Purpose and Scope

This policy defines all procedures to be followed in the event of unauthorized access, loss, theft, disclosure, or corruption of personal data, commercial information, customer data, technical logs, or other sensitive information processed or stored by Atak Domain.

This policy covers the following incidents:

- Personal data breaches
- Customer account compromises
- Unauthorized EPP/API access
- DNS or domain management account hijacking
- Unauthorized access to servers or databases
- Malware-related data breaches
- Breaches originating from third-party service providers

This policy is binding for all employees, partners, resellers, contractors, and all third parties acting as data processors.

2. Definition of Data Breach

A “data breach” refers to any of the following:

- Unauthorized access to personal data
- Loss, deletion, or corruption of data
- Transmission of data to malicious third parties
- Compromise of data integrity or security
- Any incident that requires reporting under GDPR

3. Data Breach Detection Methods

Atak Domain detects data breaches through:

- Security monitoring systems (SIEM, IDS/IPS)
- Access logs and API log anomalies
- Unusual activity in DNS/Domain transfer operations
- SOC/Cyber Security unit reports
- Customer complaints
- Firewall/WAF alerts
- DDoS statistics
- Notifications from third-party security firms or CERT/CERT-TR

Detection may be automated or manual.

4. Data Breach Assessment Criteria

To determine whether an incident constitutes a data breach, the following factors are analyzed:

- Type of compromised data (personal data, payment data, domain account)
- Number of affected individuals
- Sensitivity level of the data
- Whether the data may have been exposed, copied, or altered
- Whether the data has been used maliciously
- Whether the data has been irreversibly lost

If the incident involves personal data, GDPR Articles 33 and 34 may require reporting.

5. Data Breach Response Process

The following 6-step response process applies to all data breaches:

5.1. Detection and Validation

- The incident is initially recorded by the Cyber Security / DevOps team.
- The authenticity of the incident is verified.
- In critical cases, all operations from the moment of detection are logged.

5.2. Isolation

- The affected system is immediately isolated.
- If necessary, the relevant server is quarantined.
- EPP, API, or customer account passwords are reset.
- Unauthorized sessions are terminated.

5.3. Impact Analysis

The following questions are evaluated:

- Which data has been affected?
- Did the attacker obtain the data or only access it?
- How long was the system exposed?
- How many individuals were affected?
- Has the integrity of the system been compromised?

The results are recorded in the “Data Breach Impact Report.”

5.4. Corrective Action

- The attack vector is closed
- Security vulnerabilities are patched
- Additional security controls are applied
- Affected customer accounts are placed in secure mode
- DNS/EPP transfer locks are activated

5.5. Notification

A. If personal data is involved – GDPR and KVKK obligations

- Notification to supervisory authorities within 72 hours under GDPR
- Notification to affected users when required
- For Turkish personal data, KVKK breach notification within 72 hours

B. ICANN requirements

Under ICANN RAA 3.18, in security-related events notifications may be sent to:

- ICANN
- The relevant registry
- Official authorities requesting information when WHOIS/Proxy is used

C. Other notifications

- Banks and payment institutions
- Hosting partners
- Security vendors
- CERT / USOM / CERT-TR (for Turkey)

5.6. Closure and Reporting

- A final data breach report is prepared
- Submitted to the Board of Directors
- Legal proceedings may be initiated if required
- Preventive controls are implemented to avoid recurrence

6. Customer Notification Criteria

Customers will be notified in the following cases:

- Password, identity data, or account access information has leaked
- Domain transfer authorization has been compromised
- DNSSEC keys or nameserver data were stolen
- Whois data was accessed without authorization
- Payment data (even tokenized) is at risk

Customer notification includes:

- What happened
- When it happened
- Which data was affected
- Actions taken by Atak Domain
- Required actions for the customer
- Contact information

7. Post-Incident Recovery Plan

- Full security audit of all systems
- Penetration testing
- Improvements to logging systems

- Mandatory MFA
- Increased API rate limits
- Additional security training for employees
- Architectural modifications if needed

8. Third Parties and Resellers

All resellers, partners, technical providers, and SaaS services acting as processors on behalf of Atak Domain must:

- Notify Atak Domain of a data breach within 24 hours
- Provide all logs related to the incident
- Cooperate fully
- Comply with the Data Processing Agreement (DPA)

9. Limitation of Liability

Atak Domain is not responsible for:

- Customer errors (weak passwords, phishing, infected devices)
- Security vulnerabilities caused by third-party plugins/themes
- Breaches occurring within customer systems
- Vulnerabilities in customer-owned hosting infrastructure

10. Enforcement and Updates

This policy is effective as of the publication date.
It may be updated in response to changes in ICANN, GDPR, or national regulations.

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