SAFİ GALATA HOLDİNG ANONIM ŞIRKETI

VERİ İHLALİ MÜDAHALE PLANI
(Data Breach Response Plan)

Şirket	Safi Galata Holding A.Ş.
Yürürlük	01.04.2026
Versiyon	1.0
Hazırlayan	Hukuk ve Uyum Birimi

1. AMAÇ VE YASAL YÜKÜMLÜLÜK

Bu Plan; Safi Galata Holding Anonim Şirketi'de gerçekleşen veya şüphelenilen veri ihlallerine hızlı, koordineli ve hukuka uygun biçimde müdahale edilmesini, zararın asgariye indirilmesini ve yasal bildirim yükümlülüğünün yerine getirilmesini sağlamaktadır.

Kanun'un 12. maddesi 5. fıkrası: İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul uygulamasında fiili beklenti 72 saattir; süre ihlalden haberdar olunan andan itibaren işler.

2. MÜDAHALE EKİBİ

Rol	Birincil Sorumlu	Yedek	Görev
İhlal Koordinatörü (Lider)	Hukuk ve Uyum Müdürü	Genel Müdür Yardımcısı	Tüm süreci yönetir, Kurul bildirimi yapar
BT Güvenlik Sorumlusu	BT Müdürü	Kıdemli BT Uzmanı	Teknik analiz, ihlali sınırlandırma, log muhafazası
İK Müdürü	İK Müdürü	İK Uzmanı	Çalışan verisi içeren ihlallerde bilgilendirme
İletişim Sorumlusu	Yönetim / PR	Genel Müdür	Harici iletişim yönetimi
Üst Yönetim	Genel Müdür	Yönetim Kurulu Bşk.	Kritik karar onayı

Ekip üyelerinin 7/24 ulaşılabilir iletişim bilgileri ayrı bir gizli Ek'te saklanır ve her 6 ayda güncellenir.

3. MÜDAHALE AŞAMALARI

Aşama 0 — Tespit ve İlk Bildirim (0–4 Saat)

- İhlali tespit eden kişi derhal BT Güvenlik Sorumlusuna ve İhlal Koordinatörüne bildirir
- İhlal Kayıt Formu doldurulur: tespit tarihi/saati, türü, kapsamı
- Genel Müdür bilgilendirilir; Müdahale Ekibi toplanır

Aşama 1 — Sınırlama ve Kanıt Muhafazası (0–12 Saat)

- Sızdırılan veriye erişim sağlayan hesap ve sistemler derhal izole edilir veya devre dışı bırakılır
- İlgili tüm log kayıtları salt okunur ortama alınır ve yedeklenir — KAYITLAR SİLİNMEZ
- Harici saldırı varsa USOM ve siber güvenlik firması devreye alınır
- Adli analiz için sistem görüntüsü (snapshot) alınır

Aşama 2 — Risk Analizi (12–24 Saat)

Etkilenen veri kategorisi, kişi sayısı, ihlal türü, verinin şifreli olup olmadığı ve ihlal devam edip etmediği değerlendirilir. Risk düzeyi (Düşük / Orta / Yüksek / Kritik) belirlenerek sonraki adımlar kararlaştırılır.

Aşama 3 — Kurul Bildirimi (Azami 72 Saat)

Bildirim www.kvkk.gov.tr İhlal Bildirim Modülü üzerinden yapılır. Tam bilgi mevcut değilse kısmi bildirim yapılır, eksikler tamamlanarak ek bildirim gönderilir.

- Veri sorumlusu kimlik ve iletişim bilgileri
- İhlalin türü ve tespiti
- Etkilenen veri kategorileri ve yaklaşık kişi sayısı
- Olası sonuçlar ve alınan / alınacak tedbirler

Aşama 4 — İlgili Kişilere Bildirim

'Orta' ve üzeri risk düzeyinde etkilenen veri sahiplerine bildirim yapılır. Bildirimde: ihlal açıklaması, etkilenen veri türleri, alınan önlemler, veri sahibinin alabileceği önlemler ve iletişim bilgileri yer alır.

Aşama 5 — İyileştirme ve Sonrası

- Güvenlik açığının kalıcı olarak kapatılması ve penetrasyon testi yaptırılması
- İhlalden 30 gün sonra 'İhlal Sonrası Değerlendirme Raporu' hazırlanması
- Kök neden analizi, alınan dersler ve kalıcı önlemler
- İhlal kayıtları en az 5 yıl muhafaza edilir

4. FİDYE YAZILIMI ÖZEL PROTOKOLÜ

Fidye ödemesi kesinlikle yapılmaz. Tüm sistemler ağdan izole edilir; temiz yedekten geri yükleme yapılır; USOM ve siber güvenlik firması devreye alınır; savcılığa suç duyurusunda bulunulur; 72 saat içinde Kurul'a bildirim yapılır.

5. TATBIKAT VE EĞİTİM

- Plan yılda en az bir kez masa başı tatbikatla test edilir; sonuçlar kayıt altına alınır
- BT ve İK personeline yılda en az bir kez ihlal müdahale eğitimi verilir
- Yeni çalışanlara işe başlamada planın ilgili bölümleri aktarılır
- Plan her yıl Ocak ayında ve mevzuat değişikliklerinde gözden geçirilir