

BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ VE KAPSAM

Bu Politika'nın amacı, KÂR Katılım Altın Rafinerisi A.Ş.'nin sahip olduğu veya sorumluluğunda bulunan bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumaya ilişkin temel ilkeleri belirlemektir.

Politika; ticari sırların, müşteri ve tedarikçi bilgilerinin, kişisel verilerin, laboratuvar ve üretim kayıtlarının, finansal bilgilerin ve kurumsal sistemlerin risk temelli bir yaklaşımla korunmasını amaçlar.

Bu Politika; elektronik, basılı, sözlü, görsel veya diğer ortamlarda bulunan tüm bilgi varlıklarını; bunları işleyen kişi, süreç, uygulama, cihaz, ağ, tesis ve hizmetleri kapsar.

Yönetim Kurulu üyeleri, yöneticiler, çalışanlar, stajyerler, danışmanlar, yükleniciler, tedarikçiler ve bilgiye erişim yetkisi verilen diğer taraflar Politika'nın kendileriyle ilgili hükümlerine uyar.

2. TEMEL İLKELER VE TAAHHÜTLERİMİZ

Şirket, bilgi güvenliği yönetiminde aşağıdaki ilkeleri benimser ve taahhüt eder:

- Uygulanabilir mevzuata, kişisel verilerin korunmasına ilişkin yükümlülöklere, sözleşmelere ve Şirketin benimsediğı bilgi güvenliği gerekliliklerine uymak.
- ISO/IEC 27001:2022 kapsamında belgelendirilmiş bilgi güvenliği yönetim sistemini risk temelli bir yaklaşımla kurmak, uygulamak, sürdürmek ve sürekli iyileştirmek.
- Bilgi varlıklarını envanterlemek, sahiplerini belirlemek, hassasiyet ve iş değeri doğrultusunda sınıflandırmak ve kullanım kurallarını tanımlamak.
- Erişim yetkilerini bilmesi gereken ve asgari yetki ilkelerine göre vermek; görev değışikliğı ve işten ayrılma süreçlerinde yetkileri zamanında güncellemek veya kaldırmak.
- Kimlik doğrulama, ayrıcalıklı erişim, kayıt altına alma, ağ güvenliği, zararlı yazılımdan korunma, güvenli yapılandırma, güncelleme ve zafiyet yönetimi kontrollerini riske uygun şekilde uygulamak.
- Hassas bilgilerin iletimi, saklanması, kopyalanması, paylaşılması, fiziksel taşınması ve imhasında uygun teknik ve idari koruma tedbirleri kullanmak.
- Laboratuvar sonuçları, üretim ve izlenebilirlik kayıtları ile finansal ve ticari verilerin yetkisiz değışikliğe karşı bütünlüğünü ve gerekli süre boyunca erişilebilirliğini sağlamak.
- Yedekleme, geri dönüş testleri, iş sürekliliğı ve felaket kurtarma düzenlemeleriyle kritik süreçlerin kesinti riskini yönetmek.

- Bilgi güvenliği olaylarını bildirmek, sınıflandırmak, müdahale etmek, kanıtları korumak, etkileri azaltmak ve tekrarını önleyici faaliyetler yürütmek.
- Tedarikçi, bulut, yazılım, altyapı ve dış hizmet kaynaklı bilgi güvenliği risklerini seçim, sözleşme, erişim ve performans izleme süreçlerinde değerlendirmek.
- Fiziksel alanları, sunucu ve ağ ekipmanlarını, arşivleri ve kritik çalışma ortamlarını yetkisiz erişim, hasar ve çevresel tehditlere karşı korumak.
- Çalışanların bilgi güvenliği ve kişisel veri farkındalığını işe girişte ve düzenli eğitimlerle geliştirmek; sosyal mühendislik ve benzeri tehditlere karşı bilinç oluşturmak.

3. GÖREV VE SORUMLULUKLAR

- Yönetim Kurulu, Politikayı onaylar ve bilgi güvenliği risklerine ilişkin üst gözetimi sağlar.
- Genel Müdürlük, bilgi güvenliği yönetim sistemi için gerekli kaynak ve yetkileri sağlar; risk kabulü ve kritik iyileştirme kararlarını uygun seviyede ele alır.
- Bilgi teknolojileri ve bilgi güvenliğinden sorumlu birim; teknik kontrolleri işletir, risk değerlendirmelerini ve olay müdahalesini koordine eder, kayıt ve göstergeleri raporlar.
- Bilgi varlığı sahipleri, sorumlu oldukları bilginin sınıflandırılması, erişim şartları, saklama ihtiyacı ve uygun kullanımının belirlenmesinden sorumludur.
- Kişisel veri işleyen birimler, veri minimizasyonu, amaçla sınırlılık, saklama ve imha kurallarına uyar; ihlal şüphesini gecikmeksizin bildirir.
- Tüm kullanıcılar, kendilerine verilen erişim araçlarını korur; yetkisiz paylaşım yapmaz ve şüpheli olayları belirlenen kanallardan bildirir.

4. İZLEME, KAYIT VE GERİ BİLDİRİM

4.1. İzleme ve Kayıt

- Bilgi güvenliği performansı; olaylar, erişim gözden geçirmeleri, zafiyet ve güncelleme durumu, yedekleme ve geri dönüş testleri, eğitimler, tedarikçi kontrolleri ve düzeltici faaliyetler üzerinden izlenir.
- Risk değerlendirmeleri, iç kontroller, bağımsız testler ve yönetimin gözden geçirmesi riske ve ihtiyaçlara göre gerçekleştirilir.
- Bilgi güvenliği olay kayıtları ve deliller, gizlilik ve bütünlükleri korunarak ilgili mevzuat ve saklama kurallarına uygun biçimde muhafaza edilir.

4.2. Geri Bildirim

Etik ihlal veya uygunsuzluk şüphesi içeren bildirimlere ilişkin soru, endişe veya geri bildirimler aşağıdaki iletişim kanalları aracılığıyla iletebilir:

Etik ve İhbar Bildirimleri: etik@karaltinrafinerisi.com

Web Formu: Etik ve Uyum İhlalleri Bildirim Formu

Adres: Yarımburgaz Mah. 1. Cumhuriyet Cad. No:50 İç Kapı No: 1 Küçükçekmece / İstanbul / TÜRKİYE

Bildirimler gizlilik, tarafsızlık, kişisel verilerin korunması ve misillemeden korunma ilkeleri çerçevesinde değerlendirilir. İyi niyetli bildirimde bulunan kişiye karşı herhangi bir olumsuz işlem yapılmasına izin verilmez.

5. İHLALLER VE YAPTIRIMLAR

Bu Politika hükümlerine, Şirket politika ve prosedürlerine, etik ilkelere veya yürürlükteki mevzuata aykırı davranışlar ihlal olarak değerlendirilir. İhlalin niteliği, ağırlığı, tekrarı, etkisi ve ilgili tarafın statüsü dikkate alınarak gerekli idari, sözleşmesel ve/veya hukuki aksiyonlar değerlendirilir.

Çalışanlar bakımından, yürürlükteki iş mevzuatı, iş sözleşmeleri, etik ilkeler ve ilgili Şirket iç düzenlemeleri çerçevesinde uygun aksiyonlar alınır. Üçüncü taraflar, tedarikçiler, müşteriler, iş ortakları, hizmet sağlayıcılar ve danışmanlar bakımından ise ilgili sözleşme hükümleri, taahhütler ve Şirket prosedürleri çerçevesinde iş ilişkisinin askıya alınması, sınırlandırılması veya sona erdirilmesi dahil gerekli aksiyonlar uygulanabilir.

İhlalin niteliğine göre, gerekli hallerde yetkili kurum ve kuruluşlara bildirimde bulunulması, düzenleyici mercilere raporlama yapılması veya adli/idari mercilere başvurulması değerlendirilebilir. Şirket, iyi niyetle bildirimde bulunan kişilere karşı misilleme yapılmasını kabul etmez.

Çıkar çatışması doğuran veya doğurma ihtimali bulunan durumlarda çalışanlar, yöneticiler, Yönetim Kurulu üyeleri ve Şirket adına hareket eden ilgili taraflar, söz konusu durumu zamanında ve yazılı olarak beyan etmekle yükümlüdür. Çıkar çatışması beyanları yılda en az bir kez ve olay bazlı olarak Çıkar Çatışması Beyan Formu aracılığıyla alınır; alınan beyanlar İç Kontrol ve Tedarik Zinciri Uyum Görevlisi tarafından Çıkar Çatışması Beyan Sicilinde kayıt altına alınır, takip edilir ve gizlilik esası çerçevesinde muhafaza edilir.

6. POLİTİKANIN ERİŞİLEBİLİRLİĞİ VE ŞEFFAFLIK

Bu Politika, Şirket'in resmi internet sitesi ve uygun iletişim kanalları aracılığıyla ilgili paydaşların erişimine açık şekilde yayımlanır. Şirket, politikanın şeffaflık ilkesi doğrultusunda kamuya açık, erişilebilir ve güncel tutulmasını taahhüt eder.

İlgili Dokümanlar:

- Kişisel Verilerin Korunması Hakkında Aydınlatma Metni
- Etik ve Uyum İhlalleri Bildirim Formu
- Çıkar Çatışması Beyan Formu

- Çıkar Çatışması Beyan Sicili

7. ONAY VE YÜRÜRLÜK

İşbu Politika, 11/08/2026 tarihinde Yönetim Kurulu tarafından onaylanarak yürürlüğe girmiştir.

Politika, sorumlu birim tarafından en az yılda bir kez ve ayrıca mevzuat, standartlar, organizasyon yapısı, faaliyetler veya risk profilinde önemli değişiklik olması halinde gözden geçirilir.

Bu Politika'nın İngilizce çevirisi ile Türkçe metni arasında herhangi bir uyumsuzluk, çelişki veya yorum farklılığı bulunması halinde Türkçe metin esas alınır.

Doküman Bilgisi	Açıklama
Yönetim Kurulu Karar Tarihi	11/08/2026
Yönetim Kurulu Karar Sayısı	2026-05
Yürürlük Tarihi	11/08/2026
Versiyon No.	01
Revizyon No.	00
Doküman Kodu	POL.01
Hazırlayan	Gökçe YILMAZ – İç Kontrol ve Tedarik Zinciri Uyum Görevlisi Şerafettin KULELİ – Entegre Yönetim Sistemi Temsilcisi Nurullah KARABİBER – ISO Yönetim Sistemi Danışmanı
Onaylayan	Sercan YAŞA – Yönetim Kurulu Başkanı
Son Gözden Geçirme Tarihi	07/08/2026
Bir Sonraki Gözden Geçirme Tarihi	02/08/2027
Yayımlanma Tarihi	09/09/2026