

VERİ GİZLİLİĞİ VE BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman Kodu	OM-POL-04
Yayın Tarihi	01.01.2025
Revizyon	01
Revizyon Tarihi	.../.../.....
Kapsam	Tüm birimler, çalışanlar, yöneticiler, alt işverenler, tedarikçiler ve şirket adına hareket eden üçüncü kişiler

Yürürlük notu: Bu metin onay ve kurum içi duyuru sonrası uygulanır. Belirtilen tarih talep edilen doküman tarihidir; geçmişte yürürlükte olduğuna dair kanıt oluşturmaz.

1. Amaç ve kapsam

Bu politikanın amacı; Orhun Metal Madencilik İnşaat Sanayi ve Ticaret A.Ş.'nin ("Şirket") çalışan, çalışan adayı, alt işveren çalışanı, tedarikçi, müşteri, ziyaretçi, yerel halk ve iş ortaklarına ait kişisel verileri ile üretim, analiz, rezerv, fiyat, sözleşme, finans ve teknik bilgilerini yetkisiz erişim, değiştirme, kayıp, ifşa ve kötüye kullanıma karşı korumak; bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamaktır.

Politika; tüm saha, tesis ve ofislerde, kâğıt ve elektronik ortamdaki tüm bilgileri, Şirket bilişim sistemlerini, saha otomasyon ve kontrol sistemlerini (SCADA, PLC, kantar, laboratuvar cihazları), mobil cihazları, bulut hizmetlerini ve bu varlıkları kullanan tüm çalışan, yönetici, alt işveren, tedarikçi ve ziyaretçileri kapsar.

2. Dayanak ve ilgili dokümanlar

Bu politika başta 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve ikincil düzenlemeleri, Kişisel Verileri Koruma Kurulu kararları, 5237 sayılı Türk Ceza Kanunu (m.135–140 kişisel verilere ilişkin suçlar, m.239 ticari sırların açıklanması, m.243–245 bilişim suçları), 6102 sayılı Türk Ticaret Kanunu (m.55 haksız rekabet), 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Kanunu, 7545 sayılı Siber Güvenlik Kanunu (kapsama girilmesi halinde), 4857 sayılı İş Kanunu ve 6331 sayılı İş Sağlığı ve Güvenliği Kanunu'na dayanır. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve ISO/IEC 27701 Gizlilik Bilgi Yönetimi standartları iyi uygulama referansı olarak esas alınır (Ek-3).

Politika; OM-POL-01, OM-POL-02 ve OM-POL-03 ile Şirketin Kişisel Veri Saklama ve İmha Politikası, aydınlatma metinleri ve bilgi güvenliği talimatlarıyla birlikte uygulanır.

3. Tanımlar

- Kişisel veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi (ad-soyad, T.C. kimlik no, telefon, adres, fotoğraf, kamera kaydı, araç plakası, konum, bordro, performans kaydı vb.).
- Özel nitelikli kişisel veri:** Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler (KVKK m.6).
- İlgili kişi:** Kişisel verisi işlenen gerçek kişi.
- Veri sorumlusu:** Şirket. **Veri işleyen:** Şirket adına ve talimatıyla kişisel veri işleyen üçüncü kişiler (bordro, bulut, güvenlik, laboratuvar, OSGB, lojistik firmaları vb.).

- **Kişisel veri ihlali:** Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi veya kaybı, yok olması, değişmesi.
- **Bilgi güvenliği olayı:** Bilginin gizliliğini, bütünlüğünü veya erişilebilirliğini tehdit eden her türlü olay (siber saldırı, fidye yazılımı, yetkisiz erişim, cihaz kaybı, hatalı gönderim, sistem kesintisi vb.).

4. Roller ve sorumluluklar

- **Üst yönetim:** Politikanın sahibidir; gerekli bütçe ve kaynakları sağlar ve yıllık değerlendirme raporunu onaylar.
- **KVKK ve Bilgi Güvenliği Sorumlusu / Komitesi:** Üst yönetimce görevlendirilen hukuk, bilgi teknolojileri ve insan kaynakları temsilcilerinden oluşur; kişisel veri envanterini, VERBİS kayıtlarını, aydınlatma metinlerini, ilgili kişi başvurularını ve ihlal süreçlerini yönetir; risk değerlendirmesi yapar ve yılda en az bir kez rapor verir.
- **Bilgi teknolojileri birimi:** Teknik güvenlik tedbirlerini, erişim yetkilerini, yedeklemeyi, kayıtları (log) ve olay müdahalesini yürütür.
- **Birim yöneticileri:** Birimlerinde işlenen verilerin envantere uygun, amaçla sınırlı ve güvenli işlenmesinden; yetki taleplerinin onayından sorumludur.
- **Tüm çalışanlar:** Bu politikaya uymak, eğitimlere katılmak ve olayları derhal bildirmekle yükümlüdür.

5. Bilgi sınıflandırma ve erişim yönetimi

Bilgiler, sahibi olan birim tarafından aşağıdaki sınıflardan birine ayrılır ve buna uygun korunur:

Sınıf	Örnekler	Asgari koruma
Kamuya açık	İnternet sitesi içeriği, yayımlanmış raporlar, ilanlar	Yayın öncesi yetkili onayı
Kurum içi	Prosedürler, iç duyurular, organizasyon şemaları	Yalnızca çalışanlarla paylaşılır
Gizli	Sözleşmeler, fiyatlar, tedarikçi bilgileri, finans verileri, kişisel veriler	Bilmesi gereken prensibi, erişim kaydı, şifreli aktarım
Çok gizli	Rezerv ve tenör verileri, ihale ve satın alma stratejileri, ruhsat projeleri, özel nitelikli kişisel veriler, Yönetim Kurulu kararları	İsmlendirilmiş erişim listesi, şifreleme, çok faktörlü kimlik doğrulama, çıktı ve harici paylaşım kısıtı

- Erişim yetkileri “bilmesi gereken” ve “en az yetki” prensipleriyle, birim yöneticisinin yazılı talebi ve bilgi teknolojileri biriminin onayıyla tanımlanır.
- Her kullanıcıya kişiye özel hesap verilir; ortak hesap kullanılmaz. Yönetici (admin) yetkileri ayrı hesaplarla ve sınırlı sayıda kişiye verilir.
- Görev değişikliğinde yetkiler aynı gün güncellenir; işten ayrılıştta tüm erişimler en geç son çalışma günü kapatılır ve Şirket cihazları, kartları ve belgeleri teslim alınır.
- Kritik sistemlerdeki erişim yetkileri en az altı ayda bir birim yöneticileri tarafından gözden geçirilir.

6. Kişisel verilerin korunması

6.1. Genel ilkeler ve hukuki sebepler

Kişisel veriler, KVKK m.4 uyarınca hukuka ve dürüstlük kurallarına uygun, doğru ve gerektiğinde güncel, belirli, açık ve meşru amaçlar için, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işlenir ve amaç için gerekli süre kadar muhafaza edilir. Her işleme faaliyeti KVKK m.5 veya m.6'daki hukuki sebeplerden birine dayanır; kanunda öngörülen diğer şartlar bulunuyorsa açık rızaya başvurulmaz, açık rızanın gerektiği hallerde ise rıza hizmet şartına bağlanmaz.

6.2. Envanter, VERBİS ve aydınlatma

- Tüm birimlerin işlediği kişisel veriler; veri kategorisi, amaç, hukuki sebep, alıcı grupları, saklama süresi, yurt dışı aktarım ve güvenlik tedbirleri belirtilerek Kişisel Veri İşleme Envanteri'nde kayıt altına alınır ve yılda en az bir kez güncellenir.
- Şirket, Kurul'un belirlediği istisna kriterlerini aşması halinde Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) kaydolar ve bilgileri değişiklikten itibaren mevzuatta öngörülen süre içinde günceller.
- Çalışan, aday, ziyaretçi, tedarikçi, müşteri ve kamera kayıtları için ayrı aydınlatma metinleri hazırlanır; veri toplanırken ilgili kişiye sunulur (KVKK m.10 ve Aydınlatma Yükümlülüğü Tebliği).

6.3. Özel nitelikli kişisel veriler

- **Sağlık verileri:** İşe giriş ve periyodik muayene sonuçları, iş kazası ve meslek hastalığı kayıtları yalnızca işyeri hekimi ve yetkili sağlık personeli tarafından erişilebilecek şekilde ayrı ve kilitli/şifreli ortamda tutulur. İnsan kaynaklarına yalnızca "çalışmaya elverişli / elverişli değil" bilgisi iletilir.
- **Biyometrik veriler:** Parmak izi, yüz tanıma gibi biyometrik sistemler, ancak KVKK m.6'daki şartların bulunması ve Kurul kararları doğrultusunda kullanılabilir. Bu sistemler kullanılacaksa, açık rıza vermeyen çalışanlara kart veya şifre gibi alternatif bir giriş yöntemi sunulur.
- **Ceza mahkûmiyeti ve sendika üyeliği** gibi veriler yalnızca kanunun açıkça öngördüğü hallerde işlenir.
- Özel nitelikli kişisel veriler için Kurul'un belirlediği yeterli önlemler (ayrı erişim yetkisi, şifreleme, eğitim, gizlilik taahhüdü, log kaydı) uygulanır.

6.4. İşyerinde izleme ve kamera kayıtları

- Güvenlik kameraları yalnızca güvenlik, İSG ve varlık koruma amaçlarıyla, aydınlatma levhaları asılarak kullanılır. Tuvalet, soyunma odası, duş, ibadet ve dinlenme alanları ile özel yaşam alanları izlenmez; ses kaydı alınmaz.
- Kurumsal e-posta, internet ve bilgi sistemleri kullanımı; çalışanlar önceden açık ve anlaşılır biçimde bilgilendirilerek, yalnızca meşru bir amaçla, ölçülü ve kademeli olarak (önce otomatik ve anonim kontroller, gerektiğinde içerik incelemesi) izlenebilir. İçerik incelemesi yalnızca somut bir ihlal şüphesi halinde, hukuk biriminin onayıyla ve tutanakla yapılır.
- Araç takip (GPS) sistemleri yalnızca Şirket araçlarında, mesai süresi ve iş amacıyla sınırlı olarak kullanılır.

6.5. İlgili kişi başvuruları

İlgili kişiler KVKK m.11'deki haklarını (bilgi talep etme, düzeltme, silme, itiraz, zararın giderilmesini talep etme vb.) Şirkete yazılı olarak, kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza

veya Şirkete daha önce bildirilen ve sistemde kayıtlı e-posta adresi aracılığıyla kullanabilir.
Başvurular için iletişim bilgileri:

- E-posta: info@orhunmetal.com
- Telefon (bilgi için): +90 533 446 01 52

Başvurular, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde, kural olarak ücretsiz sonuçlandırılır (KVKK m.13). Başvuru sahibinin kimliği doğrulanmadan bilgi verilmez. Başvurular ve verilen yanıtlar kayıt altına alınır.

7. Dijital güvenlik

- **Kimlik doğrulama:** Parolalar en az 12 karakter ve karmaşık olur, kişiye özeldir, paylaşılmaz ve yazılı olarak saklanmaz. E-posta, uzaktan erişim (VPN), bulut, bankacılık ve yönetici hesaplarında çok faktörlü kimlik doğrulama zorunludur.
- **Güncelleme ve koruma:** İşletim sistemleri ve yazılımlar güncel tutulur; güvenlik yamaları kritik olanlar için en geç 14 gün içinde uygulanır. Tüm uç noktalarda zararlı yazılım koruması ve disk şifrelemesi kullanılır; lisanssız veya onaysız yazılım yüklenmez.
- **Ağ güvenliği:** Güvenlik duvarı, misafir ağının kurum ağından ayrılması, kablosuz ağ şifrelemesi ve uzaktan erişimde yalnızca Şirket VPN'i kullanılır. İnternet hizmeti sunulan alanlarda 5651 sayılı Kanun ve ilgili yönetmelik kapsamındaki iç IP dağıtım kayıtları mevzuatta öngörülen süre boyunca saklanır.
- **Kayıt (log) yönetimi:** Kritik sistemlerde erişim ve işlem kayıtları tutulur, değiştirilemez biçimde saklanır ve düzenli olarak incelenir.
- **Yedekleme ve iş sürekliliği:** Kritik veriler düzenli olarak, en az bir kopyası çevrim dışı veya değiştirilemez ortamda ve farklı bir lokasyonda olacak şekilde yedeklenir; yedekten geri dönüş testi en az altı ayda bir yapılır. Fidyе yazılımı ve sistem kesintisi senaryolarını içeren iş sürekliliği planı hazırlanır.
- **Saha otomasyon sistemleri (OT):** Cevher hazırlama tesisi kontrol sistemleri, kantar ve laboratuvar cihazları kurum ağından ayrıştırılır; uzaktan bakım erişimleri yalnızca kayıtlı, süreli ve onaylı bağlantılarla verilir. Bu sistemlerdeki güvenlik açıkları İSG riski olarak da değerlendirilir.
- **E-posta ve ortalama:** Şüpheli bağlantı ve ekler açılmaz; para transferi, banka hesap değişikliği veya şifre talebi içeren e-postalar ikinci bir kanaldan teyit edilmeden işleme alınmaz (OM-POL-03 Bölüm 5).
- **Mobil cihazlar ve taşınabilir medya:** Şirket verisi içeren mobil cihazlarda ekran kilidi ve uzaktan silme özelliği etkin tutulur. USB bellek vb. taşınabilir medya yalnızca onaylı ve şifreli olarak kullanılır.
- **Bulut ve yapay zekâ araçları:** Şirket verileri yalnızca bilgi teknolojileri birimince onaylanmış bulut hizmetlerinde saklanır. Gizli ve çok gizli bilgiler ile kişisel veriler, Şirketçe onaylanmamış çevrimiçi yapay zekâ, çeviri veya dosya dönüştürme araçlarına yüklenmez.
- **Uzaktan çalışma:** Uzaktan çalışmada yalnızca Şirket cihazları ve VPN kullanılır; ekranın başkalarının görülmesi engellenir, ortak alanlarda gizli görüşme yapılmaz.

8. Fiziksel güvenlik

- Sunucu odası, arşiv, laboratuvar, numune deposu, kantar ve patlayıcı deposu gibi kritik alanlara giriş kartlı veya kayıtlı olarak yalnızca yetkili kişilerce yapılır.
- Ziyaretçiler kayıt altına alınır, kart verilir ve refakatle dolaştırılır.
- Temiz masa ve temiz ekran kuralı uygulanır: Masadan ayrılırken ekran kilitlenir; gizli belgeler masada, yazıcıda veya ortak alanlarda bırakılmaz ve kilitli dolaplarda saklanır.

- Kâğıt belgeler kırıcıda veya imha firmasınca tutanakla; elektronik medya ve cihazlar ise verinin geri getirilemeyeceği yöntemlerle imha edilir.
- Saha görüntüleri, drone çekimleri, haritalar ve sondaj verileri yetkisiz kişilerle ve sosyal medyada paylaşılmaz.

9. Üçüncü taraflar ve veri paylaşımı

- Laboratuvar, lojistik, müşteri, OSGB, bordro, bilişim, güvenlik ve diğer hizmet sağlayıcılarla veri paylaşımı iş ihtiyacıyla ve gerekli en az veriyle sınırlandırılır.
- Veri işleyenlerle KVKK m.12/2 uyarınca veri güvenliği yükümlülüklerini, alt veri işleyen kullanımını, ihlal bildirimini, denetim hakkını ve sözleşme sonunda verilerin iadesi veya imhasını düzenleyen veri işleme sözleşmesi imzalanır. Tedarikçilerle gizlilik sözleşmesi yapılır.
- Kişisel veriler kamu kurumlarına yalnızca yasal bir talep veya yükümlülük üzerine, yetkili kişi onayıyla ve talep edilen kapsamla sınırlı olarak verilir.
- **Yurt dışına aktarım:** Yurt dışında sunucusu bulunan bulut, e-posta ve yazılım hizmetleri dahil, kişisel verilerin yurt dışına aktarılması yalnızca KVKK m.9 ve Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'teki şartlara uygun yapılır: yeterlilik kararı bulunması; bulunmaması halinde Kurul'ca ilan edilen standart sözleşme gibi uygun güvencelerden birinin sağlanması ya da istisnai (arızı) aktarım hallerinden birinin varlığı. Standart sözleşmeler imzalanmasından itibaren beş iş günü içinde Kurum'a bildirilir.

10. Gizli ticari bilgiler

- Rezerv, tenör, sondaj sonuçları, fiyat, maliyet, müşteri ve tedarikçi bilgileri ile ihale ve ruhsat projeleri ticari sır niteliğindedir; görev süresince ve sonrasında yetkisiz kişilerle paylaşamaz. Bu yükümlülük iş sözleşmelerine ve gizlilik taahhütnamelerine eklenir.
- Ticari sırların yetkisiz açıklanması TCK m.239 ve TTK m.55 kapsamında cezai ve hukuki sorumluluk doğurur.
- Kamuya açıklama ve basın açıklamaları yalnızca yetkilendirilmiş kişilerce yapılır.

11. Bilgi güvenliği olayları ve kişisel veri ihlali yönetimi

Yanlış alıcıya gönderim, cihaz veya belge kaybı, yetkisiz erişim, fidye yazılımı, şüpheli e-posta tıklaması veya diğer siber olay şüphesinde çalışan durumu derhal amirine ve bilgi teknolojileri birimine bildirir. Olay bildirimini gecikmeksizin yapılır; bildirimde bulunan çalışana, kendi hatası olsa dahi, iyi niyetle yaptığı bildirim nedeniyle yaptırım uygulanmaz.

- **Sınırlama:** Etkilenen hesaplar ve cihazlar ağdan ayrılır, şifreler değiştirilir, delil niteliğindeki kayıtlar korunur.
- **Değerlendirme:** KVKK ve Bilgi Güvenliği Komitesi, olayın kişisel veri ihlali olup olmadığını, etkilenen kişi ve veri kategorilerini ve olası sonuçlarını değerlendirir.
- **Kurul'a bildirim:** Kişisel veri ihlali, KVKK m.12/5 ve Kurul'un 2019/10 sayılı kararı uyarınca, öğrenilmesinden itibaren gecikmeksizin ve en geç 72 saat içinde Kişisel Verileri Koruma Kurulu'na Kurum'un ihlal bildirim formuyla bildirilir; gecikme halinde gerekçesi de sunulur.
- **İlgili kişilere bildirim:** Etkilenen kişilerin tespitinden sonra makul en kısa sürede ilgili kişilere doğrudan, mümkün değilse uygun yöntemlerle bildirim yapılır.
- **Diğer bildirimler:** Siber olaylarda 7545 sayılı Siber Güvenlik Kanunu kapsamındaki yükümlülükler (kapsama girilmesi halinde), suç şüphesi bulunan hallerde adli makamlara başvuru ve sigorta bildirimleri değerlendirilir.

- **Kayıt ve iyileştirme:** Tüm olaylar, ihlal müdahale kaydına işlenir; kök neden analizi yapılır ve düzeltici faaliyetler uygulanır.

12. Saklama, imha ve denetim

- Kişisel veriler, ilgili mevzuatta öngörülen veya işleme amacının gerektirdiği süre kadar saklanır; süre sonunda silinir, yok edilir veya anonim hale getirilir. Şirket, VERBİS kayıt yükümlüsü olması halinde Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca Kişisel Veri Saklama ve İmha Politikası hazırlar ve periyodik imhayı en fazla altı aylık aralıklarla yapar. İmha işlemleri tutanakla kayıt altına alınır ve en az üç yıl saklanır.
- Örnek saklama süreleri Ek-1'de yer alır; kesin süreler Kişisel Veri Saklama ve İmha Politikası'nda belirlenir.
- Erişim hakları, yedekleme, log kayıtları ve veri işleyen sözleşmeleri periyodik olarak kontrol edilir. Bilgi güvenliği uygulamaları yılda en az bir kez iç denetimden geçirilir; kritik sistemler için düzenli zafiyet taraması ve gerektiğinde sızma testi yaptırılır.

13. Eğitim ve farkındalık

Tüm çalışanlara işe girişte ve en az yılda bir kez KVKK ve bilgi güvenliği eğitimi verilir; ortalama farkındalık testleri yapılır. İnsan kaynakları, İSG, muhasebe, satın alma, güvenlik ve bilgi teknolojileri gibi yoğun kişisel veri işleyen birimlere ek eğitim verilir. Çalışanlardan ve kişisel veriye erişen alt işveren personelinden gizlilik taahhütnamesi alınır (Ek-2).

14. İhlallerin sonuçları

Bu politikaya aykırılık, iş mevzuatı ve disiplin düzenlemeleri çerçevesinde yaptırıma tabidir. Kişisel verilere ve bilişim sistemlerine ilişkin ihlaller ayrıca TCK m.135–140 ve m.243–245 kapsamında cezai sorumluluk, KVKK m.18 kapsamında Şirket için idari para cezası ve ilgili kişilere karşı tazminat sorumluluğu doğurabilir.

15. Sorumluluk, gözden geçirme ve yürürlük

Üst yönetim politikanın sahibidir; KVKK ve Bilgi Güvenliği Komitesi koordinasyondan, ilgili birim yöneticileri uygulama, kayıt ve eğitimlerden sorumludur. Politika en az yılda bir kez ve önemli mevzuat, teknoloji veya operasyon değişikliklerinde gözden geçirilir. İlgili kayıtlar mevzuat ve Şirketin saklama kurallarına göre muhafaza edilir. Bu politika onay ve kurum içi duyuru tarihinde yürürlüğe girer.

Ek-1: Örnek saklama süreleri

Kayıt türü	Örnek saklama süresi	Dayanak / gerekçe
Personel özlük dosyası	İş ilişkisinin sona ermesinden itibaren 10 yıl	TBK m.146 genel zamanaşımı; 4857 m.75
Bordro, puantaj, SGK bildirimleri	10 yıl	TTK m.82; 5510 sayılı Kanun
İşyeri hekimi kişisel sağlık dosyaları	En az 15 yıl; kanserojen/mutajen madde ve asbest maruziyetinde 40 yıl	İSG mevzuatı
İş kazası ve İSG kayıtları	En az 15 yıl	İSG mevzuatı; olası tazminat davaları
Muhasebe ve ticari belgeler	10 yıl	TTK m.82
Vergi kayıtları	5 yıl (zamanaşımı süresince)	VUK m.253

Kayıt türü	Örnek saklama süresi	Dayanak / gerekçe
İş başvuru formları ve CV'ler (işe alınmayan)	6 ay – 1 yıl	Amaçla sınırlılık
Güvenlik kamerası kayıtları	30 gün (olay halinde sonuçlanana kadar)	Amaçla sınırlılık
Ziyaretçi kayıtları	1 yıl	Güvenlik
İç IP dağıtım kayıtları	Mevzuatta öngörülen süre	5651 sayılı Kanun ve yönetmelik
İlgili kişi başvuruları ve ihlal kayıtları	10 yıl	İspat yükü; zamanaşımı

Ek-2: Gizlilik ve bilgi güvenliği taahhütnamesi

OM-POL-04 Veri Gizliliği ve Bilgi Güvenliği Politikası'nı okuduğumu ve anladığımı; görevim nedeniyle eriştiğim kişisel verileri ve gizli bilgileri yalnızca görevimin gerektirdiği amaçla kullanacağımı, görevim süresince ve sona ermesinden sonra yetkisiz kişilerle paylaşmayacağımı; şifrelerimi kimseyle paylaşmayacağımı ve fark ettiğim her bilgi güvenliği olayını derhal bildireceğimi; aksi davranışın disiplin, hukuki ve cezai sorumluluk doğurabileceğini bildiğimi beyan ederim.

Adı Soyadı	
Görevi / Birimi	
Tarih	
İmza	

Ek-3: İlgili mevzuat ve referanslar

Alan	Mevzuat ve referanslar
Kişisel veriler	6698 sayılı Kişisel Verilerin Korunması Kanunu; Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik; Veri Sorumluları Sicili Hakkında Yönetmelik; Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik; Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ; Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ; Kişisel Verileri Koruma Kurulu kararları (özel nitelikli veriler için yeterli önlemler, ihlal bildirimi)
Bilişim ve siber güvenlik	7545 sayılı Siber Güvenlik Kanunu; 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve toplu kullanım sağlayıcılara ilişkin yönetmelik
Ceza ve ticaret hukuku	5237 sayılı Türk Ceza Kanunu (m.135–140, 239, 243–245); 6102 sayılı Türk Ticaret Kanunu (m.55, 82)
Çalışma hayatı ve İSG	T.C. Anayasası (m.20, 22); 4857 sayılı İş Kanunu (m.75); 6331 sayılı İş Sağlığı ve Güvenliği Kanunu ve ilgili yönetmelikler
Standartlar	ISO/IEC 27001; ISO/IEC 27701; ISO 22301 İş Sürekliliği

Revizyon geçmişi

Rev.	Tarih	Açıklama
00	01.01.2025	İlk yayın.
01	.../.../.....	Kapsam, dayanak, tanımlar ve roller eklendi; dört seviyeli bilgi sınıflandırma tablosu, KVKK envanter-VERBİS-aydınlatma, özel nitelikli veriler (sağlık, biyometrik), işyerinde izleme ve kamera, ilgili kişi başvuruları ve iletişim bilgileri, ayrıntılı dijital ve fiziksel güvenlik tedbirleri (MFA, yedekleme, OT güvenliği, yapay zekâ araçları), veri işleyen sözleşmeleri ve 2024 değişiklikleri sonrası yurt dışı aktarım, 72 saatlik ihlal bildirimi, saklama-imha, eğitim ve yaptırımlar ile Ek-1 saklama süreleri, Ek-2 taahhütname ve Ek-3 mevzuat listesi eklendi.

HAZIRLAYAN	ONAYLAYAN
Kübra Kartal İmza: _____	Çise Ergüden İstanbullu İmza: _____