

## MAPA GRUP & MNG GRUP DİJİTAL GÜVENLİK VE GİZLİLİK POLİTİKASI

### 1. Giriş

**Mapa Grup** ve **MNG Grup** (bundan böyle **Mapa İnşaat ve Ticaret A.Ş.** dahil olmak üzere "**Grup**" olarak anılacaktır) olarak, dijitalleşmenin giderek daha fazla hakim olduğu günümüz iş dünyasında dijital güvenlik ve gizliliğin kritik öneminin farkındayız. Bu **Dijital Güvenlik ve Gizlilik Politikası**, hassas bilgilerin korunması, dijital varlıkların bütünlüğünün sağlanması ve bireylerin gizlilik haklarının korunması konusundaki kararlılığımızı özetlemektedir.

*Grup, uyum gerekliliklerinin sektör, coğrafya ve iş modeli gibi faktörlere bağlı olarak değişebileceğini kabul eder. Bu Politikada özetlenen ana ilkelere **bağlı kalmakla birlikte, Grup bünyesindeki münferit şirketler, iştirakler, bağlı ortaklıklar ve kuruluşlar, kendi ticari faaliyetlerinde karşılaştıkları riskleri ve zorlukları ele alarak kendileri için uygun ve etkili olan kendi uyum politikalarını ve prosedürlerini geliştirme ve uygulama yetkisine sahiptir. Bu esneklik ve özerklik, Grup'un genel hedefleri ve değerleri ile uyumu sağlar ve uyum konusunda özel yaklaşımlara olanak tanır.***

### 2. Hedefler

Grup'un Dijital Güvenlik ve Gizlilik Politikasının hedefleri şunlardır:

- a. Veri Koruma:** Tüm dijital varlıkları ve hassas bilgileri yetkisiz erişim, ifşa, değiştirme ve imhaya karşı korunması.
- b. Uyumluluk:** İlgili veri koruma yasalarına, yönetmeliklerine ve endüstri standartlarına uygunluğun sağlanması.
- c. Gizlilik:** Şeffaf veri uygulamaları ve onay mekanizmaları uygulayarak bireylerin gizlilik haklarının korunması.

### 3. Bilgi Güvenliği Yönetim Sistemi (BGYS)

Grup, özellikle ISO/IEC 27001 olmak üzere uluslararası standartlara dayalı bir Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamayı ve sürdürmeyi taahhüt etmektedir. Kapsamı, Grup bünyesindeki şirketler için BT departmanında yürütülen yazılım geliştirme ve bilgi teknolojileri teknik ve altyapı desteği kapsamındaki bilgi güvenliği faaliyetlerine yoğunlaşmıştır. BGYS, dijital güvenlik hedeflerine ulaşmak için temel teşkil eder.

### 4. Veri Koruma

- a. Erişim Kontrolleri:** Hassas verilere yalnızca yetkili personelin erişebilmesini sağlamak için sağlam erişim kontrolleri uygulamak
- b. Şifreleme:** Verilerin hem aktarım sırasında hem de beklemede korunması için şifreleme mekanizmalarından yararlanmak
- c. Olay Müdahalesi:** Güvenlik olaylarını derhal ele almak ve etkilerini azaltmak için bir olay müdahale planı oluşturmak

### 5. Uyumluluk

- a. Yasal Gereklilikler:** Gelişen veri koruma yasaları ve yönetmelikleriyle uyumluluğu sağlamak için politikaları düzenli olarak gözden geçirmek ve güncellemek

**b. Çalışan Eğitimi:** Dijital güvenlik ve gizlilik düzenlemelerini daha iyi anlamalarını sağlamak için çalışanlara sürekli eğitim vermek

**c. Üçüncü Taraf Uyumluluğu:** Üçüncü taraf tedarikçilerden, alt yüklenicilerden ve iş ortaklarından dijital güvenlik ve gizlilik standartlarına ve geçerli veri koruma yasalarına ve yönetmeliklerine uymalarını talep etmek.

## 6. Veri Gizliliği

**a. Şeffaflık:** Veri toplama ve işleme amaçları da dahil olmak üzere veri uygulamaları hakkında bireyleri açıkça bilgilendirmek.

**b. Onay:** Kişisel bilgileri toplamadan veya işlemeyen önce açık ve bilgilendirilmiş onay almak.

**c. Veri Minimizasyonu:** Yalnızca amaçlanan amaç için gerekli olan minimum miktarda kişisel bilgi toplamak ve işlemek.

## 7. Siber Güvenlik

**a. Ağ Güvenliği:** Siber tehditlere ve yetkisiz erişime karşı koruma sağlamak için sağlam ağ güvenliği önlemleri uygulamak.

**b. Güvenlik Farkındalığı:** Eğitim programları ve düzenli güncellemeler yoluyla çalışanlar arasında bir güvenlik bilinci kültürünü teşvik etmek

**c. Güvenlik Açığı Yönetimi:** İstismarı önlemek için dijital sistemlerdeki güvenlik açıklarını düzenli olarak değerlendirmek ve ele almak.

## 8. Olay Raporlama

**a. Raporlama Prosedürleri:** Çalışanların şüpheli veya gerçek güvenlik olaylarını derhal bildirmeleri için açık prosedürler oluşturmak.

**b. Soruşturma:** Temel nedenleri belirlemek ve düzeltici önlemleri uygulamak için bildirilen olaylara ilişkin kapsamlı soruşturmalar yürütmek.

## 9. İzleme ve Denetleme

**a. Sürekli İzleme:** Güvenlik tehditlerini gerçek zamanlı olarak tespit etmek ve bunlara yanıt vermek için dijital sistemlerin sürekli izlenmesini sağlamak.

**b. Düzenli Denetimler:** Dijital Güvenlik ve Gizlilik Politikasının ve ilgili kontrollerin etkinliğini değerlendirmek için düzenli denetimler gerçekleştirmek.

## 10. Çalışan Sorumluluğu

**a. Veri İşleme Eğitimi:** Çalışanları dijital bilgilerin sorumlu bir şekilde ele alınması ve gizliliğin önemi konusunda eğitmek.

**b. Hesap verebilirlik:** Çalışanları dijital güvenlik ve gizlilik politikaları ve prosedürlerine uyma konusunda sorumlu tutmak.

## 11. Bildirim ve İhbar

Grup açık konuşma yaklaşımını benimsemekte ve çalışanlara ve paydaşlara bu Dijital Güvenlik ve Gizlilik Politikası da dahil olmak üzere uyum politikalarımızla ilgili etik veya yasal ihlalleri veya endişeleri bildirmeleri için kanallar sağlamaktadır. Bu kanallar gizlilik,

anonimlik ve misillemeye karşı koruma sağlar. Grup bildirimleri derhal ve şeffaf bir şekilde ele almaya kararlıdır.

- Grup, tüm çalışanları endişe ve önerilerini bunları uygun şekilde ele alabilecek üstleriyle paylaşmaya teşvik eder.
- Grup <https://mapagroup.etikmerkezi.com> adresinden çevrimiçi olarak veya +908502304568'den telefonla erişilebilen bir **Etik Destek Merkezi** kurmuştur. Etik Destek Merkezi, yürürlükteki yasaların sınırları dahilinde Grup için bildirim sürecinin gizliliğini, güvenliğini ve anonimliğini temin eden bağımsız bir üçüncü taraf sağlayıcı tarafından sağlanmaktadır.  
Tüm çalışanlarımızı, tedarikçilerimizi, alt yüklenicilerimizi, iş ortaklarımızı, müşterilerimizi ve ticari faaliyetlerimizden etkilenen yerel toplulukların bireylerini Etik Destek Merkezi'ni kullanmaya teşvik ediyoruz.
- Ayrıca, uyum ve etik görevlilerimize doğrudan telefonla (tüm şantiye ve ofis çalışanlarımız ile iş ortaklarımıza verilen telefon numaralarını arayarak) veya [complianceaudit@mapa.group](mailto:complianceaudit@mapa.group) adresine e-posta göndererek ulaşılabilir.

İsimsiz veya başka bir şekilde iyi niyetle yapılan bildirimler, herhangi bir soruşturmanın sonucuna bakılmaksızın derhal ve misilleme korkusu olmaksızın ele alınacaktır.

## 12. Gözden Geçirme ve Sürekli İyileştirme

- Gözden Geçirme:** Dijital Güvenlik ve Gizlilik Politikasının etkinliğini periyodik olarak gözden geçirmek ve değerlendirmek.
- Sürekli İyileştirme:** Ortaya çıkan tehditleri ele almak ve Grup'un iş hedefleriyle uyumu sağlamak için gerekli iyileştirmeleri uygulamak.

Bu Dijital Güvenlik ve Gizlilik Politikası, Grup'un en yüksek dijital güvenlik standartlarını sürdürme, bireylerin gizliliğini koruma ve tüm paydaşlar için güvenli ve güvenilir bir dijital ortamı teşvik etme taahhüdünü yansıtmaktadır.

**EK**  
**MAPA GRUP & MNG GRUP**  
**DİJİTAL GÜVENLİK VE GİZLİLİK POLİTİKASINA**  
**UYUMA DAİR KABUL VE ONAY**

**Mapa Grup & MNG Grup Dijital Güvenlik ve Gizlilik Politikasını** bütünüyle inceledim ve anladım. İşbu belge ile Grup'a, bu Dijital Güvenlik ve Gizlilik Politikasını ihlal etmediğimi onaylıyorum ve bu Politikada belirtilen tüm etik standartlara uymayı taahhüt ediyorum.

Grup'un bir çalışanı olarak, bu Dijital Güvenlik ve Gizlilik Politikasının herhangi bir ihlalinin, benim için geçerli olduğu ölçüde, geçerli prosedür gerekliliklerine ve ilgili yasalara tabi olarak sözlü veya yazılı uyarılar, mevki düşürme, transfer veya işten çıkarma gibi uygun disiplin cezalarıyla sonuçlanacağını anladığımı da teyit ederim. Bilinen veya makul ölçüde şüphelenilen herhangi bir ihlalin bildirilmemesinin bile kendi başına disiplin cezasına yol açabileceğinin farkındayım.

Grup'un bir tedarikçisi/alt yüklenicisi/iş ortağı olarak, işbu Dijital Güvenlik ve Gizlilik Politikasının herhangi bir şekilde ihlal edilmesinin, benim için geçerli olduğu ölçüde, Grup ile olan iş ve sözleşme ilişkimin sona ermesine neden olabileceğini ve yürürlükteki yasalar uyarınca bana karşı hukuki ve cezai yaptırım uygulanabileceğini anladığımı teyit ederim.

Gelecekte ortaya çıkabilecek ve bu Dijital Güvenlik ve Gizlilik Politikasına uygun olarak ifşa edilmesini gerektiren her türlü durumu derhal bildireceğimi taahhüt ederim.

Tarih: \_\_\_\_\_

İmza: \_\_\_\_\_

İsim: \_\_\_\_\_

Ünvan: \_\_\_\_\_