

# GÜVENLİK POLİTİKASI

## Get Energy

Yürürlük tarihi: 07 Temmuz 2026

Parametre	Bilgiler
Hizmet operatörü	ŞARJAL TİCARET ŞİRKETİ LİMİTED
Hizmetin ticari adı	Get Energy
Tescil numarası	MŞ28752
Elektronik şirket numarası	102944933544
Adres	Beşparmaklar Cad. Nazım Bodi Plaza No:4 Çatalköy Girne, TRNC
Web sitesi	getenergy.energy
E-posta	info@getenergy.energy

### 1. Genel hükümler

1.1. İşbu Güvenlik Politikası, ŞARJAL TİCARET ŞİRKETİ LİMİTED şirketinin Get Energy hizmetini sunarken kullanıcıları, ödemeleri, verileri, kiralama istasyonlarını, ekipmanı ve hizmetin dijital altyapısını korumak amacıyla uyguladığı temel organizasyonel, teknik ve usule ilişkin güvenlik önlemlerini belirler.

1.2. Get Energy, kullanıcılara web sitesi, QR kod, ödeme sayfası, mevcut olması halinde mobil uygulama ve Şirket tarafından desteklenen diğer dijital kanallar aracılığıyla taşınabilir şarj cihazlarını kiralama imkanı sunar. Temel kiralama, belirli bir işlem, güvenlik kontrolü, ödeme sağlayıcısı gerekliliği veya uyumsuzluğun çözümü için açıkça gerekli olmadıkça, zorunlu hesap kaydı olmadan gerçekleştirilebilir.

1.3. İşbu Politika, Get Energy yasal belgelerinin genel paketinin bir parçasıdır ve Kullanıcı Sözleşmesi, Gizlilik Politikası, Kiralama Politikası, Tarife Kuralları, İade Politikası, Ödeme ve Otomatik Tahsilat Kuralları, Ekipman Bedeli Tazmin Politikası ve hizmetin diğer belgeleri ile birlikte uygulanır.

1.4. Politikanın amacı, hizmetin işleyişinde hangi güvenlik önlemlerinin uygulandığını, kullanıcıdan hangi davranışların beklendiğini ve Şirketin tehditlere, olaylara, hileli işlemlere, teknik arızalara ve hizmetin hukuka aykırı kullanım girişimlerine nasıl tepki verdiğini kullanıcılara ve iş ortaklarına açıklamaktır.

### 2. Uygulama alanı

2.1. Politika, Get Energy hizmetinin tüm dijital ve fiziksel bileşenlerine uygulanır. Bunlara web sitesi, kiralama sayfaları, ödeme sayfaları, QR kodları, kiralama istasyonları, taşınabilir şarj cihazları, iç idari paneller, teknik destek, ödeme süreçleri ve kullanıcı başvurularının işlenmesi dahildir.

2.2. Politika; QR kod veya web sitesi üzerinden zorunlu kayıt olmaksızın kiralama başlatan kullanıcılara, hesap sahibi kullanıcılara, Şirket çalışanlarına ve yüklenicilerine, ayrıca hizmetin sunulmasına katılan teknik ve ödeme tedarikçilerine uygulanır.

2.3. İşbu Politika, hizmet güvenliği açısından risk yaratabilecek dahili teknik ayrıntıları açıklamaz. Gizli anahtarlar, sunucu yapılandırmaları, dahili adresler, oturum açma bilgileri, altyapı yönetim süreçleri ve sınırlı erişimli diğer bilgiler bu kapsama dahildir.

### 3. Temel güvenlik ilkeleri

- uygulanan güvenlik önlemlerinin hukuka uygun, şeffaf ve ölçülü olması;
- işlenen verilerin ve erişim yetkilerinin asgari düzeyde tutulması;
- ödemelerin korunması ve yetkisiz işlemlerin önlenmesi;
- idari ve teknik fonksiyonlara erişimlerin ayrılması;
- veri aktarımında güvenli iletişim kanallarının kullanılması;
- istasyonların ve dijital servislerin çalışabilirliğinin sürekli kontrol edilmesi;
- arızaların ve uyuşmazlıkların araştırılması için önemli teknik olayların kaydedilmesi;
- güvenlik olaylarına ve kullanıcı başvurularına zamanında yanıt verilmesi;
- kayıtsız kiralama kolaylığı ile gerekli güvenlik seviyesi arasında denge kurulması.

3.2. Şirket, kullanıcının ekipmanı hızlı şekilde kiralayabileceği, ancak ödeme, ekipman teslimi, iade, ekipman bedeli tahsilatı veya para iadesi ile bağlantılı her işlemin teknik olarak doğrulanabileceği ve bir uyuşmazlık doğduğunda kontrol edilebileceği bir hizmet tasarımı hedefler.

### 4. Zorunlu kayıt olmadan kiralamanın güvenliği

4.1. Zorunlu kayıt olmadan web üzerinden kiralama, kullanıcının kalıcı bir hesap oluşturmadan QR kod, istasyon sayfası veya ödeme sayfası üzerinden kiralama başlatabilmesi anlamına gelir. Bu model kullanıcı kolaylığı için uygulanır ve kiralama başlamadan önce hizmetin yasal belgelerinin kabul edilmesi gerekliliğini ortadan kaldırmaz.

4.2. Hesap bulunmasa dahi hizmet, kiralama gerçeğinin doğrulanması, belirli işlemin belirli ekipmanla ilişkilendirilmesi, ekipmanın iadesi, bedelin hesaplanması ve dolandırıcılığın önlenmesi için gerekli teknik ve ödeme tanımlayıcılarını işleyebilir.

4.3. Şirket; güvenlik, dolandırıcılığın önlenmesi, uyuşmazlığın çözümü, iade işlemi, ekipmanın iade edilmemesinin araştırılması veya ödeme kuruluşu gerekliliklerinin yerine getirilmesi için gerekli olduğunda ek bilgi, telefon numarası doğrulaması, e-posta adresi doğrulaması, ödeme kontrolü veya hesap oluşturulmasını talep edebilir.

4.4. Zorunlu kaydın bulunmaması, ödeme işleminin anonim olduğu anlamına gelmez. Ödemeler; bankalar, ödeme sistemleri, ödeme servisleri ve kendi doğrulama ve güvenlik prosedürlerini uygulayan diğer ödeme katılımcıları tarafından işlenebilir.

### 5. Ödeme güvenliği

5.1. Get Energy, ödeme anında kullanıcıya sunulan banka kartları, Apple Pay, Google Pay ve diğer desteklenen ödeme yöntemleri dahil olmak üzere mevcut ödeme yöntemleriyle ödeme kabul eder. Ödemeler, hizmete bağlı ödeme sağlayıcıları, bankalar ve ödeme kuruluşları aracılığıyla işlenir.

5.2. Şirket, hizmetin sunulması için gerekli olmayan tam banka kartı numarasını, kart güvenlik kodunu ve diğer tam ödeme bilgilerini saklamaz. Tam ödeme bilgilerinin işlenmesi, kendi ödeme verisi güvenliği standartlarını uygulayan ödeme sağlayıcısı, banka veya ödeme servisi tarafında gerçekleştirilir.

5.3. Güvenlik amacıyla ödeme işlemi; ön provizyon, geçici fon blokesi, 3D Secure doğrulaması, kullanıcının bankası üzerinden onay, ödeme aracının tokenleştirilmesi, başarısız ödeme halinde yeniden tahsilat denemesi ve ödeme kuruluşu tarafından öngörülen diğer kontrolleri içerebilir.

5.4. Apple Pay veya Google Pay kullanıldığında, kartın gerçek bilgileri genellikle bir ödeme tokeniyle değiştirilir ve işlem onayı ödeme servisi ile kullanıcının cihazı üzerinden yapılır. Şirket yalnızca işlemin doğrulanması, kiralamanın ifası ve olası uyuşmazlıkların çözümü için gerekli bilgileri alır.

Önlem	Açıklama
Ödeme onayı	Ekipman verilmeden önce bankanın, ödeme sağlayıcısının veya ödeme servisinin ödeme işlemini kontrol etmesi.
Ön provizyon	Kiralama bedelinin, olası sonraki tahsilatların veya ekipman bedeli tazmininin güvence altına alınması için tutarın geçici olarak bloke edilmesi.
3D Secure	Bu doğrulama uygulanıyorsa, kullanıcının banka veya ödeme servisi üzerinden işlemi ek olarak onaylaması.
Ödeme tokeni	Şirket tam kart verilerini saklamadan, kiralama koşulları kapsamında sonraki tahsilatların yapılabilmesini sağlayan ödeme aracına ilişkin teknik tanımlayıcı.
Yeniden tahsilat denemesi	İşlem başarısız olduğunda, hizmet ve ödeme kuruluşu kuralları izin veriyorsa ödeme sağlayıcısına yeniden başvurulması.

## 6. QR kodlarının ve kiralama sayfalarının güvenliği

6.1. QR kodları kullanıcıyı belirli bir istasyon, istasyon gözü, kiralama sayfası veya ödeme sayfası ile ilişkilendirmek için kullanılır. Kullanıcı, QR kodu taradıktan sonra Get Energy sayfasına veya hizmet tarafından belirtilen başka bir resmi ödeme kanalına yönlendirildiğini kontrol etmelidir.

6.2. Şirket, kullanıcıya; alan adı yazımında hata bulunan, güvenli bağlantı kullanmayan, şüpheli görünen veya resmi hizmet arayüzüne görsel olarak uymayan sayfalara ödeme bilgisi girmemesini tavsiye eder.

6.3. Kullanıcı, zarar görmüş QR kod etiketi, orijinal kodun üzerine yapıştırılmış yabancı bir kod, şüpheli ödeme sayfası veya Get Energy resmi süreci dışında ödeme talep eden bir mesaj tespit ederse işlemi durdurmalı ve destek birimine başvurmalıdır.

6.4. Şirket; kod değişikliği, teknik arıza, yetkisiz müdahale veya diğer güvenlik tehditleri belirtileri tespit edildiğinde QR kodlarını, istasyonları veya belirli istasyon gözlerini engelleme ya da geçici olarak devre dışı bırakma hakkına sahiptir.

## 7. İstasyonların ve ekipmanın güvenliği

7.1. Get Energy istasyonları, taşınabilir şarj cihazlarının otomatik olarak verilmesi ve geri alınması için tasarlanmıştır. Her teslim ve iade işlemi istasyonun teknik araçları, yazılımı ve olay günlükleri ile kaydedilebilir.

7.2. Ekipman, belirli bir cihazı belirli bir kiralama işlemi, teslim istasyonu, iade istasyonu, teslim zamanı ve iade zamanı ile ilişkilendirmeye olanak sağlayan benzersiz tanımlayıcılara sahip olabilir.

7.3. Kullanıcı, istasyona ve ekipmana özenli davranmak, gövdeyi açmamak, yapısını değiştirmemek, tanımlayıcıları kaldırmamak, teslim veya iade mekanizmasını aşmaya çalışmamak ve hizmetin güvenliğini bozabilecek işlemler yapmamakla yükümlüdür.

7.4. Ekipman hasarlı, aşırı ısınmış, açılmış, yanık kokusu bulunan, gövdesi deforme olmuş, konnektörü zarar görmüş veya başka açık bir kusur içeriyor görünüyorsa kullanıcı kullanımı durdurmalı, güvenli ise ekipmanı istasyona iade etmeli ve destek birimini bilgilendirmelidir.

7.5. Şirket; hasar, yanlış iade, teknik hata, dolandırıcılık veya kullanıcı güvenliği tehdidi belirtileri tespit edildiğinde ekipmanı ya da istasyonu geçici olarak bloke edebilir.

## 8. Kişisel verilerin ve teknik verilerin korunması

8.1. Şirket, kişisel ve teknik verileri Gizlilik Politikası uyarınca işler. Güvenlik kapsamında ödeme, kiralama, istasyon, ekipman, tarayıcı, cihaz, işlem zamanı, teknik hata, ağ olayı ve kullanıcı başvurularına ilişkin bilgiler işlenebilir.

8.2. Güvenlik verileri; işlemlerin doğrulanması, dolandırıcılığın önlenmesi, ödemelerin korunması, uyuşmazlıkların araştırılması, hizmetin çalışabilirliğinin kontrol edilmesi ve yasal gerekliliklerin yerine getirilmesi amacıyla kullanılır.

8.3. Şirket asgari veri ilkesini uygular: veriler, belirli amaç için gerekli olan ölçüde toplanır ve saklanır. Verilere erişim yalnızca görev veya sözleşme yükümlülüklerinin yerine getirilmesi için gerekli olan kişi ve sistemlere verilir.

8.4. Verilerin üçüncü kişilere aktarımı yalnızca hizmetin yasal belgelerinde, uygulanabilir mevzuatta, kullanıcıyla yapılan sözleşmede, ödeme kuruluşu gerekliliklerinde veya yetkili makamın yasal talebinde öngörülen hallerde mümkündür.

## 9. Güvenli veri aktarımı

9.1. Kullanıcı, web sitesi, ödeme sayfası ve sunucu altyapısı arasında veri aktarımı için ilgili hizmet bileşeni destekliyse HTTPS/TLS dahil güvenli iletişim kanalları kullanılır.

9.2. Kullanıcı; tarayıcı güvenli olmayan bağlantı, geçersiz sertifika, site taklidi veya başka bir güvenlik riski hakkında uyarı verdiğinde ödeme bilgisi girmeye devam etmemelidir.

9.3. Şirket, hizmet veya kullanıcılar için artan risk oluşturan eski, güvensiz ya da desteklenmeyen tarayıcı, cihaz, yazılım veya ağ istemcilerine erişimi sınırlayabilir.

9.4. Hizmet bileşenleri arasındaki dahili veri aktarımı ayrıca erişim ayırımı, dahili anahtarlar, ağ kısıtlamaları, günlükleme ve bütünlük kontrolü gibi teknik araçlarla korunabilir.

## 10. Erişim yönetimi

10.1. Get Energy idari sistemlerine çalışanların, yüklenicilerin ve teknik tedarikçilerin erişimi ihtiyaç ve asgari yeterli erişim ilkesiyle sağlanır.

10.2. Şirket; bireysel hesaplar, rol ayırımı, işlem günlükleri, fonksiyon bazlı erişim sınırlaması, erişim haklarının periyodik kontrolü ve işbirliğinin sona ermesi veya görev değişikliği halinde erişimin geri alınması gibi yöntemler uygulayabilir.

10.3. Ödeme işlemlerine, kişisel verilere, güvenlik günlüklerine, tarife ayarlarına, istasyon yönetimine ve iade işlemlerine erişim sınırlı sayıda yetkili kişiye verilmelidir.

10.4. Çalışanlar ve yükleniciler gizlilik rejimine uymak, hesap bilgilerini üçüncü kişilere aktarmamak, erişimi görev gereği dışında kullanmamak ve şüpheli olayları gecikmeksizin bildirmekle yükümlüdür.

İlke	Pratik anlamı
Asgari erişim	İç sistemdeki her kullanıcı yalnızca kendi fonksiyonları için gerekli hakları alır.
Yetki ayrımı	Ödemeler, tarifeler, istasyonlar ve iadelerle ilgili işlemler farklı roller arasında ayrılabilir.
Günlükleme	İdari sistemlerdeki önemli işlemler kontrol ve soruşturma amacıyla kaydedilebilir.
Erişimin geri alınması	İşten ayrılma, rol değişikliği, sözleşmenin sona ermesi veya ihlal tespiti halinde erişim sona erdirilmelidir.

## 11. Olay günlükleri ve izleme

11.1. Güvenliği sağlamak amacıyla Şirket; kiralama, ödemeler, ekipmanın teslimi ve iadesi, teknik hatalar, idari sistemlerdeki işlemler, hizmete yapılan talepler ve kullanıcı başvuruları ile ilgili olay günlükleri tutabilir.

11.2. Olay günlükleri; hataların teşhisi, dolandırıcılığın önlenmesi, kiralama veya iade gerçeğinin doğrulanması, ödeme uyuşmazlıklarının araştırılması, Şirketin ve kullanıcıların haklarının korunması, ayrıca ödeme kuruluşları ve mevzuat gerekliliklerinin yerine getirilmesi için kullanılır.

11.3. Olay günlükleri, kullanıcıyı gereksiz şekilde izlemek amacıyla tutulmaz. İçerikleri, güvenlik ve hizmetin düzgün çalışması için gerekli bilgilerle sınırlıdır.

11.4. Günlüklerin saklama süreleri; işleme amaçları, mevzuat gereklilikleri, olası ödeme uyuşmazlığı süreleri, muhasebe saklama süreleri ve Şirket haklarının korunması ihtiyacı dikkate alınarak belirlenir.

## 12. Dolandırıcılığın ve hukuka aykırı kullanımın önlenmesi

12.1. Şirket; dolandırıcılık, hizmetin kötüye kullanılması, kiralama bedelinin ödenmemesi girişimleri, otomatik tahsilatların aşılması girişimleri, QR kodlarının değiştirilmesi, başkasına ait ödeme aracının kullanılması, ekipmanın hasar görmesi veya iade edilmemesi gibi durumları tespit etmek ve önlemek için önlemler uygular.

12.2. Artan risk belirtileri arasında birden fazla başarısız ödeme, daha önce uyuşmazlık konusu olmuş ödeme araçlarının tekrar kullanımı, sonrasında sıkça itiraz edilen işlemler, olağan dışı kiralama girişimleri, istasyona müdahale, ekipmanın iadesinde şüpheli davranış veya işlemin teknik verilerinde tutarsızlık bulunabilir.

12.3. Artan risk tespit edildiğinde Şirket; ekipman teslimini reddedebilir, ek doğrulama talep edebilir, hizmete erişimi sınırlayabilir, işlemi geçici olarak bloke edebilir, kiralamayı iptal edebilir, bilgileri ödeme sağlayıcısına aktarabilir veya yeterli neden varsa yetkili makamlara başvurabilir.

12.4. Güvenlik önlemleri riskin niteliğiyle orantılı olarak uygulanır ve iyi niyetli kullanıcıları haksız şekilde sınırlama amacı taşımaz.

## 13. Güvenlik olaylarına müdahale

13.1. Güvenlik olayı; hizmetin, ödemelerin, kullanıcı verilerinin, istasyonların, ekipmanın veya Şirketin iç altyapısının gizliliğini, bütünlüğünü ya da erişilebilirliğini etkileyebilecek olaydır.

13.2. Bu tür olaylara yetkisiz erişim, ödeme sayfasının taklit edilmesi, QR kodunun değiştirilmesi, kitlesel teknik hatalar, veri sızıntısı, zararlı faaliyet, istasyonun zarar görmesi, tarifelerin yetkisiz değiştirilmesi, ödeme işlemede arıza veya önemli risk doğuran başka bir olay dahil olabilir.

13.3. Bir olay halinde Şirket şu önlemleri alabilir: erişimin sınırlandırılması, istasyonun veya sayfanın devre dışı bırakılması, kiralamanın geçici olarak durdurulması, şüpheli işlemlerin iptali, ödeme sağlayıcısının bilgilendirilmesi, verilerin geri yüklenmesi, günlüklerin kontrolü, etkilenen kullanıcıların bilgilendirilmesi ve gerektiğinde yetkili makamlara başvuru.

13.4. Şirketin müdahale önceliği kullanıcıların, ödemelerin, verilerin, ekipmanın ve hizmet sürekliliğinin korunmasıdır.

Aşama	İçerik
Tespit	İzleme sistemi, kullanıcı başvurusu, banka bildirim, teknik kontrol veya iç denetimden sinyal alınması.
Değerlendirme	Kapsamın, etkilenen işlemlerin, kullanıcılar ve ödemeler üzerindeki olası etkinin belirlenmesi.
Lokalizasyon	Erişimin kısıtlanması, sorunlu bileşenin devre dışı bırakılması, şüpheli işlem veya istasyonun bloke edilmesi.
Kurtarma	Hizmetin normal çalışmaya döndürülmesi, veri bütünlüğünün ve ödeme işlemlerinin doğruluğunun kontrol edilmesi.
Analiz	Nedenlerin incelenmesi, prosedürlerin düzeltilmesi, güvenlik önlemlerinin iyileştirilmesi ve sonucun belgelendirilmesi.

## 14. Kullanıcının güvenliğe ilişkin yükümlülükleri

14.1. Kullanıcı; cihazını, tarayıcısını, ödeme aracını, telefon numarasını, e-posta adresini ve hizmetle etkileşim kurmak için kullandığı diğer araçları güvenli şekilde kullanmaktan sorumludur.

14.2. Kullanıcı aşağıdakilerle yükümlüdür:

- yalnızca resmi Get Energy web sitesini, resmi kiralama sayfalarını ve ödeme sayfalarını kullanmak;
- ödeme bilgilerini girmeden önce sayfa adresini kontrol etmek;
- kiralama veya ödeme üzerinde kontrol sağlayan bilgileri üçüncü kişilere aktarmamak;
- sahibinin izni olmadan başkasına ait banka kartı veya ödeme aracı kullanmamak;
- ödeme, geçici blokaj, otomatik tahsilat veya ekipman iade mekanizmasını aşmaya çalışmamak;
- şüpheli sayfaları, sahte QR kodlarını, hatalı ödemeleri, arızalı istasyonu veya hasarlı ekipmanı derhal Şirkete bildirmek;
- ekipmanı çalışır durumdaki bir istasyona iade etmek ve böyle bir imkan varsa hizmet arayüzünden kiralamanın tamamlandığını kontrol etmek.

14.3. Kullanıcı açık güvenlik uyarılarını görmezden gelir, sahte sayfaya veri girer, ödeme aracını üçüncü kişilere verir veya hizmeti aşan işlemler yaparsa Şirketin zararı önleme veya para iadesi sağlama imkanı sınırlı olabilir.

## 15. Resmi iletişim kanalları ve dolandırıcılık mesajlarına karşı koruma

15.1. Başvurular için resmi e-posta adresi info@getenergy.energy adresidir. Şirket ayrıca resmi web sitesinde veya hizmet arayüzünde belirtilen diğer destek kanallarını kullanabilir.

15.2. Şirket kullanıcıdan tam kart numarası, kart güvenlik kodu, banka uygulaması şifresi, bankanın tek kullanımlık kodu, e-posta giriş bilgileri veya üçüncü bir kişinin kullanıcının ödeme aracına erişmesine imkan verecek diğer bilgileri talep etmemelidir.

15.3. Kullanıcı, kiralamayı yabancı bir bağlantı üzerinden ödemeyi, kişisel hesaba para göndermeyi, doğrulama kodu paylaşmayı, bilinmeyen bir uygulama yüklemeyi veya cihaza uzaktan erişim sağlamayı teklif eden mesajlara karşı dikkatli olmalıdır.

15.4. Kullanıcı şüpheli bir mesaj aldığı anda etkileşimi durdurmalı ve bilgiyi Get Energy destek birimine göndermelidir.

## 16. Kullanıcı cihazının kaybolması veya ele geçirilmesi

16.1. Kullanıcı telefonunu, banka kartını, ödeme servisine erişimi bulunan cihazını kaybederse veya ödeme aracına üçüncü kişilerin eriştiğini düşünürse, ödeme aracının bloke edilmesi için derhal bankası veya ödeme servisi ile iletişime geçmelidir.

16.2. Bu durum aktif bir Get Energy kiralamasıyla bağlantılıysa kullanıcı, mümkün olan en kısa sürede Şirketi bilgilendirmeli ve kiralamaya ilişkin mevcut bilgileri belirtmelidir: tarih, saat, istasyon, ödeme, işlem numarası, kullanıldıysa e-posta adresi veya telefon numarası.

16.3. Şirket, teknik imkanları dahilinde işlemin kontrolü, kiralama kapsamında sonraki işlemlerin sınırlandırılması, kiralamanın tamamlanmasına yardım edilmesi veya ödeme sağlayıcısına bilgi aktarılması dahil makul önlemler alabilir.

## 17. Yedekleme ve kurtarma

17.1. Şirket, hizmetin çalışmasının geri yüklenmesi, işlemlerin doğrulanması, ödeme uyuşmazlıklarının, iadelerin ve teknik hata incelemelerinin yürütülmesi için gerekli veri ve ayarların yedeklenmesini uygulayabilir.

17.2. Yedek kopyalar içeriklerine uygun şekilde korunur ve yalnızca hizmeti geri yüklemek, iş sürekliliğini sağlamak, yasal yükümlülükleri yerine getirmek ve Şirket ile kullanıcıların haklarını korumak için kullanılır.

17.3. Yedek kopyaların saklama süreleri teknik gereklilik, güvenlik gereklilikleri ve ilgili veri kategorilerinin saklama süreleri dikkate alınarak belirlenir.

## 18. Tedarikçi ve yüklenici güvenliği

18.1. Hizmeti sunmak için Şirket; bulut altyapısı sağlayıcıları, ödeme sağlayıcıları, istasyon bakım yüklenicileri, geliştiriciler, teknik destek hizmetleri, muhasebe, hukuk ve diğer profesyonel danışmanları dahil edebilir.

18.2. Tedarikçiler ve yükleniciler yalnızca ilgili hizmetin yerine getirilmesi için gerekli veri ve sistemlere erişmelidir. Şirket onlardan gizlilik ve makul güvenlik önlemlerine uyulmasını talep edebilir.

18.3. Ödeme işleme güvenliği, banka kontrolleri, 3D Secure doğrulaması, Apple Pay ve Google Pay işlemleri bakımından ilgili kısımlarda işlemde yer alan ödeme kuruluşları ve servisler de sorumluluk taşır.

## 19. Sınırlamalar ve mutlak garanti bulunmaması

19.1. Şirket makul güvenlik önlemleri uygular; ancak hiçbir dijital sistem, ödeme sistemi, iletişim ağı, kiralama istasyonu veya kullanıcı cihazı tüm olası risklere karşı mutlak şekilde korunamaz.

19.2. Şirket, hizmetin her zaman kesintisiz, hatasız, dış arızalardan, üçüncü kişi eylemlerinden, bağlantı sorunlarından, bankacılık gecikmelerinden veya Şirketin makul kontrolü dışındaki diğer durumlardan bağımsız çalışacağını garanti etmez.

19.3. Bir güvenlik hatası, teknik arıza veya ödeme sorunu kullanıcıyı etkilerse Şirket, başvuruyu İade Politikası, Ödeme ve Otomatik Tahsilat Kuralları ve Şikayetlerin İncelenmesi Usulü dahil ilgili hizmet belgelerinde belirlenen şekilde inceler.

## 20. Zafiyetlerin ve şüpheli olayların bildirilmesi

20.1. Potansiyel bir zafiyet, QR kod değişikliği, şüpheli ödeme sayfası, ekipman teslim hatası, hatalı tahsilat veya başka bir güvenlik sorunu tespit eden kullanıcı, iş ortağı veya üçüncü kişi bunu info@getenergy.energy adresine bildirebilir.

20.2. Bildirimde olayın tarih ve saati, sayfa adresi, istasyon numarası veya konumu, sorunun açıklaması, varsa ekran görüntüleri, tam kart verisi paylaşmadan ödemeye ilişkin bilgiler ve geri dönüş için iletişim bilgisi belirtilmesi tavsiye edilir.

20.3. Sorunu bildiren kişi, tespit ettiği zafiyeti başkalarının verilerine erişmek, ödemeyi aşmak, istasyona müdahale etmek, ödeme yapmadan ekipman almak, hizmetin çalışmasını bozmak veya gizli bilgileri yaymak için kullanmamalıdır.

## 21. Güvenlik başvurularının incelenmesi

21.1. Güvenlik başvuruları olayın niteliği ve kullanıcı, ödemeler, ekipman ve hizmet üzerindeki olası etkisi dikkate alınarak incelenir. Ödemeler, aktif kiralama, ekipmanın iade edilmemesi, dolandırıcılık şüphesi, veri sızıntısı veya kullanıcı güvenliği tehdidi ile ilgili başvurular öncelik alır.

21.2. Başvurunun kontrolü için Şirket işlemi tanımlamak amacıyla ek bilgi talep edebilir, ancak kullanıcıdan tam kart numarası, kart güvenlik kodu, banka şifresi veya tek kullanımlık doğrulama kodu talep etmemelidir.

21.3. İnceleme sonucunda teknik düzeltme, ödeme iadesi veya düzeltmesi, istasyon ya da ekipman blokesi, bilgilerin ödeme sağlayıcısına aktarılması, güvenlik prosedürlerinin güncellenmesi veya durumun başka makul bir şekilde çözülmesi söz konusu olabilir.

## 22. Güvenlik Politikasının değiştirilmesi

22.1. Hizmet işlevleri, kiralama modeli, ödeme altyapısı, ödeme kuruluşu gereklilikleri, teknik güvenlik önlemleri, mevzuat veya Şirketin iç prosedürleri değişirse Şirket işbu Güvenlik Politikasını değiştirme hakkına sahiptir.

22.2. Politikanın güncel sürümü Get Energy web sitesinde yayımlanır. Yeni sürüm yürürlüğe girdikten sonra hizmetin kullanılmaya devam edilmesi, kullanıcının güncellenmiş koşulları hizmet kullanımıyla ilgili olduğu ölçüde öğrenmiş olduğu anlamına gelir.

## 23. İletişim bilgileri

23.1. Güvenlik, şüpheli mesajlar, QR kodlarının değiştirilmesi, ödeme riskleri, teknik olaylar ve veri koruması ile ilgili konularda kullanıcı Get Energy ile info@getenergy.energy e-posta adresi üzerinden iletişime geçebilir.

23.2. Başvuru yapılırken tam banka kartı numarası, kart güvenlik kodu, banka şifresi, tek kullanımlık doğrulama kodları veya üçüncü kişilerin ödeme işlemi yapmasına imkan verebilecek diğer bilgiler gönderilmemelidir.

## Ek 1. Hizmetin güvenli kullanımı için kısa kurallar

1. QR kodu yalnızca Get Energy istasyonu üzerinde tarayın ve ödeme yapmadan önce sayfa adresini kontrol edin.
2. Şüpheli görünen veya güvenli bağlantı kullanmayan sayfalara ödeme bilgisi girmeyin.
3. Tek kullanımlık banka kodlarını ve kart bilgilerini kimseyle paylaşmayın.
4. Sahibinin izni olmadan başkasına ait ödeme aracını kullanmayın.
5. Ekipmanın gerçekten istasyon tarafından verildiğini ve kiralamanın doğru başladığını kontrol edin.
6. Ekipmanı iade ettikten sonra, bu fonksiyon varsa hizmet arayüzünde kiralamanın sona erdiğinden emin olun.
7. Hasarlı istasyon, sahte QR kodu, hatalı tahsilat veya şüpheli mesaj hakkında destek birimine bildirim yapın.
8. Ekipmanı açmayın, yapısını değiştirmeyin ve kiralama koşullarını aşarak üçüncü kişilere devretmeyin.
9. Telefonunuzu veya kartınızı kaybederseniz derhal bankanız veya ödeme servisiniz ile iletişime geçin.
10. Destek ve ödeme için yalnızca resmi Get Energy kanallarını kullanın.

## Ek 2. Temel güvenlik önlemleri matrisi

Alan	Temel önlemler
Ödemeler	Ödeme sağlayıcıları, ön provizyon, 3D Secure, tokenleştirme, banka kontrolleri.
QR kodları	Resmi sayfalara bağlantı, şüpheli kodları bloke edebilme, kullanıcı şikayetlerinin kontrolü.
İstasyonlar	Teslim ve iade işlemlerinin kaydı, arızalı istasyonların devre dışı bırakılması, uyumsuzluk konusu işlemlerin kontrolü.
Ekipman	Cihaz tanımlayıcıları, kiralama işlemi ile bağlantı, iade ve bedel tazmini kuralları.
Veriler	Minimizasyon, erişim ayırımı, güvenli aktarım, olay günlükleri.
Kullanıcı	Sayfa adresinin kontrolü, ödeme aracının korunması, şüpheli olayların bildirilmesi.
Destek	Başvuruların alınması, işlemlerin kontrolü, ödeme kuruluşları ve teknik ekiplerle etkileşim.
Olaylar	Tespit, lokalizasyon, kurtarma, neden analizi ve prosedürlerin iyileştirilmesi.

### Ek 3. Güvenlik amacıyla yasaklanan eylemler

Kullanıcıları, ödemeleri, istasyonları, ekipmanı ve verileri korumak amacıyla aşağıdaki eylemler yasaktır. Liste sınırlı değildir; Şirket, hizmet, kullanıcılar, ödemeler veya ekipman için risk yaratan diğer eylemleri de güvenlik ihlali olarak değerlendirebilir.

Yasaklanan eylem	Açıklama
QR kodunun değiştirilmesi	Resmi QR kodunun üzerine başka bir etiket yapıştırılması, kodun değiştirilmesi, kullanıcının yabancı bir sayfaya yönlendirilmesi veya benzer bir ödeme sayfası oluşturulması.
Ödemeyi aşma	Onaylanmış ödeme olmadan ekipman alma girişimi, ön provizyon veya otomatik tahsilat sürecine müdahale.
İstasyona müdahale	Gövdeyi açma, kilide zarar verme, ekipmanı zorla çıkarma, elektriği kesme veya istasyonun çalışmasına başka şekilde müdahale.
Ekipmana müdahale	Gövdeyi açma, tanımlayıcıları kaldırma, yapıyı değiştirme, parçaları değiştirme veya hasarı gizlemeye çalışma.
Başkasına ait ödeme aracını kullanma	Başka bir kişinin kartı, ödeme servisi veya banka aracılığıyla onun rızası olmadan ödeme yapma.
Yanlış başvuru	İade, arıza, ödeme, ekipman kaybı veya uyumsuzluk konusu işlem hakkında gerçeğe aykırı bilgi verme.
Toplu otomatik talepler	Web sitesi, kiralama sayfaları, ödeme sayfaları veya teknik arayüzler üzerinde aşırı yük oluşturma.
Hizmetin çalışmasını bozma	Yetkisiz erişim elde etme, kiralama verilerini, tarifeleri, ödeme durumlarını veya ekipman iade kayıtlarını değiştirme girişimi.

### Ek 4. Şirketin talep etmediği bilgiler

Kullanıcıları dolandırıcılığa karşı korumak amacıyla Şirket, Get Energy destek birimine yapılan olağan başvurularda kullanıcının banka hesabını, kartını, ödeme servisini veya kişisel hesaplarını üçüncü kişilerin yönetmesine imkan veren bilgilerin gönderilmemesi gerektiğini hatırlatır.

Bilgi veya işlem	Açıklama
Kart güvenlik kodu	Şirket, banka kartının üç veya dört haneli güvenlik kodunu talep etmez.
Tek kullanımlık banka kodu	Şirket, banka veya ödeme servisi tarafından gönderilen doğrulama kodlarını talep etmez.
Banka şifresi	Şirket, banka uygulaması, internet bankacılığı veya ödeme servisi şifresini talep etmez.
Tam kart numarası	Bir başvurunun incelenmesi için genellikle kartın son haneleri, işlem numarası veya ödeme fişindeki bilgiler yeterlidir; tam kart bilgilerinin açıklanması gerekmez.
Cihaza erişim	Şirket, ödeme veya para iadesi işlemi için uzaktan erişim programlarının kurulmasını istemez.
Kişisel hesaba ödeme	Şirket, kiralama bedelinin çalışanların, temsilcilerin veya üçüncü kişilerin kişisel hesaplarına gönderilmesini istemez.

### Son hükümler

İşbu Güvenlik Politikası yukarıda belirtilen tarihte yürürlüğe girer ve uygulanabilir mevzuatın zorunlu hükümleri, ödeme kuruluşu kuralları veya kullanıcı ya da iş ortağı ile yapılmış ayrı yazılı sözleşme tarafından aksi öngörülmedikçe Get Energy hizmeti üzerinden gerçekleştirilen tüm işlemlere uygulanır.