

	BİLGİ GÜVENLİĞİ POLİTİKAMIZ	Doküman No: CRN- POL- 001- WEB
		Rev. No: 00 Yay. Tar: 11.05.2026
		Sayfa: 1 / 4

Revizyon Tarihçesi

Rev. No	Tarih	Yapılan Değişiklik	Hazırlayan
00	11.05.2026	İlk yayın.	—

Bilgi Güvenliği Politikamız

Ceren Net Bilişim Telekomünikasyon Haberleşme İletişim Limited Şirketi ("Cerennet") olarak; abonelerimize sunduğumuz internet servis sağlayıcılığı hizmetinin güvenli, kesintisiz ve mahremiyete saygılı şekilde sürdürülmesini en önemli önceliklerimizden biri olarak görüyoruz.

Bu doğrultuda; bilgi varlıklarımızın gizliliğini, bütünlüğünü ve erişilebilirliğini koruyan ISO/IEC 27001:2022 standardına ve ilgili tüm yasal düzenlemelere uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurduk ve sürdürüyoruz.

1. Taahhütlerimiz

Cerennet olarak bilgi güvenliği konusunda aşağıdaki taahhütleri veriyoruz:

- Abonelerimize ait kişisel ve hizmet bilgilerinin yetkisiz erişime, ifşaya ve değişikliğe karşı korunması
- İnternet hizmetimizin kesintisiz, yüksek erişilebilirlikte ve güvenilir biçimde sunulması
- Yasal yükümlülüklerimize (5651 sayılı Kanun, KVKK, Elektronik Haberleşme Kanunu, BTK düzenlemeleri) tam uyum sağlanması
- Bilgi güvenliği risklerinin sistematik olarak değerlendirilmesi ve kabul edilebilir seviyede tutulması
- Bilgi güvenliği olaylarına hızlı tespit, müdahale ve etkili çözüm sağlanması
- Çalışanlarımızın ve iş ortaklarımızın bilgi güvenliği farkındalığının sürekli artırılması
- Bilgi Güvenliği Yönetim Sistemi'mizin sürekli olarak iyileştirilmesi

2. Temel İlkelerimiz

Cerennet, bilgi güvenliği yönetiminde aşağıdaki temel ilkeleri benimser:

- Gizlilik:** Bilgilere yalnızca yetkili kişilerin erişebilmesini sağlarız.
- Bütünlük:** Bilgilerin doğruluğunu ve tamlığını koruruz; yetkisiz değişikliklere karşı önlem alırız.
- Erişilebilirlik:** Bilgilerimizin ve hizmetlerimizin yetkili kullanıcılar tarafından ihtiyaç duyulduğunda kullanılabilir olmasını sağlarız.
- Yasal Uyumluluk:** İlgili tüm yasal mevzuat ve sözleşmesel yükümlülüklerle uyarız.

Hazırlayan	Onaylayan
Bilgi Güvenliği Sorumlusu	Genel Müdür

	BİLGİ GÜVENLİĞİ POLİTİKAMIZ	Doküman No: CRN- POL- 001- WEB
		Rev. No: 00 Yay. Tar: 11.05.2026
		Sayfa: 2 / 4

- **Risk Temelli Yaklaşım:** Güvenlik tedbirlerimizi varlık değeri ve risk seviyesi gözeterek belirleriz.
- **Sorumluluk Bilinci:** Tüm çalışanlarımız, görev alanlarındaki bilgi varlıklarının güvenliğinden sorumludur.
- **Sürekli İyileştirme:** BGYS'mizi düzenli olarak gözden geçirir ve geliştiririz.

3. Uyguladığımız Güvenlik Tedbirleri

Bilgi güvenliği taahhütlerimizi yerine getirebilmek için aşağıdaki temel alanlarda kapsamlı güvenlik tedbirleri uyguluyoruz:

3.1. Personel Güvenliği

- Tüm çalışanlarımızla gizlilik sözleşmesi imzalarız.
- Bilgi güvenliği farkındalık eğitimlerini düzenli olarak veririz.
- Bilgi güvenliği rol ve sorumluluklarını çalışma süreçlerimize entegre ederiz.

3.2. Erişim Güvenliği

- Sistemlerimize erişim "en az ayrıcalık" ilkesi gözetilerek verilir.
- Her kullanıcıya kişiselleştirilmiş hesap tanımlanır; ortak hesap kullanımı yasaktır.
- Erişim yetkileri düzenli olarak gözden geçirilir.
- Güçlü parola politikaları uygulanır.

3.3. Fiziksel Güvenlik

- Merkez ofis, kolokasyon alanı ve POP noktalarımız yetkisiz erişime karşı korunur.
- Kritik alanlara giriş kayıt altına alınır ve yasal süre boyunca saklanır.
- Kesintisiz güç kaynağı ve iklimlendirme sistemleri ile altyapımızın sürekliliği sağlanır.

3.4. Veri Koruma ve Yedekleme

- Kritik verilerimizin düzenli yedekleri alınır ve farklı lokasyonlarda saklanır.
- Yedeklerin geri yüklenebilirliği periyodik olarak test edilir.
- Sistem ve güvenlik kayıtları (loglar) yasal sürelerle uygun olarak muhafaza edilir.
- 5651 sayılı Kanun kapsamındaki trafik kayıtları zaman damgalı olarak korunur.

3.5. Tedarikçi Yönetimi

- Hizmet aldığımız kritik tedarikçilerle bilgi güvenliği ve gizlilik şartları içeren yazılı sözleşmeler imzalarız.
- Tedarikçi hizmet seviyelerini ve güvenlik uyumlarını düzenli olarak takip ederiz.

3.6. Olay Yönetimi

Hazırlayan	Onaylayan
Bilgi Güvenliği Sorumlusu	Genel Müdür

	BİLGİ GÜVENLİĞİ POLİTİKAMIZ	Doküman No: CRN- POL- 001- WEB
		Rev. No: 00 Yay. Tar: 11.05.2026
		Sayfa: 3 / 4

- Bilgi güvenliği olaylarını hızla tespit eder ve müdahale ederiz.
- Mevzuat gereği bildirim yapılması gereken olayları ilgili kurumlara zamanında bildiririz.
- Her olay sonrası kök neden analizi yapar, tekrarını önlemek için tedbir alırız.

3.7. İş Sürekliliği

- Kritik hizmetlerimiz için iş sürekliliği planları hazırlar ve düzenli olarak test ederiz.
- Yedek altyapı ve felaket kurtarma çözümleri ile hizmet kesintilerini en aza indiririz.

4. Uyduğumuz Standart ve Mevzuat

Bilgi Güvenliği Yönetim Sistemimiz aşağıdaki standart ve mevzuat çerçevesinde işletilmektedir:

- ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Standardı
- Bilgi ve İletişim Güvenliği Rehberi (BİGR)
- Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Kanunu
- 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)
- 5809 sayılı Elektronik Haberleşme Kanunu
- Bilgi Teknolojileri ve İletişim Kurumu (BTK) düzenlemeleri

5. Sorumluluklar

Bilgi güvenliği, Cerennet'in tüm paydaşlarının ortak sorumluluğudur:

- Üst Yönetim:** Bilgi güvenliği politikamızı onaylar, gerekli kaynakları sağlar ve örnek davranış sergileyerek bilgi güvenliği kültürünün yerleşmesine öncülük eder.
- Bilgi Güvenliği Sorumlusu:** BGYS'nin günlük yönetiminden, politika ve prosedürlerin uygulanmasından sorumludur.
- Çalışanlarımız:** Bilgi güvenliği politikamıza ve prosedürlerimize uyar; sorumluluğundaki bilgi varlıklarını korur; bilgi güvenliği olaylarını derhal bildirir.
- Tedarikçilerimiz ve İş Ortaklarımız:** Bizimle imzalanan sözleşmedeki bilgi güvenliği ve gizlilik şartlarına uyar.

6. Sürekli İyileştirme

Bilgi Güvenliği Yönetim Sistemimizi; iç tetkikler, dış denetimler, risk değerlendirmesi sonuçları, ölçüm ve izleme verileri ile yönetim gözden geçirme çıktıları temel alınarak sürekli olarak iyileştiriyoruz. Bu kapsamda tespit edilen iyileştirme alanları için düzeltici ve önleyici faaliyetler tanımlanır, uygulanır ve etkinliği izlenir.

7. Yürürlük ve Gözden Geçirme

Hazırlayan	Onaylayan
Bilgi Güvenliği Sorumlusu	Genel Müdür

	BİLGİ GÜVENLİĞİ POLİTİKAMIZ	Doküman No: CRN- POL- 001- WEB
		Rev. No: 00 Yay. Tar: 11.05.2026
		Sayfa: 4 / 4

Bu politika, Cerennet Genel Müdürü tarafından onaylanmıştır ve yürürlüktedir. Politika; mevzuat değişiklikleri, önemli bilgi güvenliği olayları, organizasyonel veya teknolojik değişiklikler, denetim bulguları veya yönetim gözden geçirme kararları doğrultusunda en az yılda bir kez gözden geçirilir.

İletişim

Bilgi güvenliği politikamız hakkında sorularınız veya bildirimleriniz için bizimle aşağıdaki kanallar üzerinden iletişime geçebilirsiniz:

İletişim Kanalı	Bilgi
Adres	Topraklık Mah. 571 Sk. No: 3/B Pamukkale / DENİZLİ
Telefon	0 258 300 0 258
E-posta	iletisim@cerennet.com.tr
Web Sitesi	https://www.cerennet.com.tr
Müşteri Paneli	https://www.cerennet.com.tr (Abone Giriş)

Cerennet
Genel Müdürlük

Hazırlayan	Onaylayan
Bilgi Güvenliği Sorumlusu	Genel Müdür