Revizyon Tarihçesi

Rev. No	Tarih	Yapılan Değişiklik	Hazırlayan
00	12.05.2026	İlk yayın.	BG Sorumlusu

1. Amaç

Bu politikanın amacı, Sarıkayanet Telekomünikasyon San. Tic. Ltd. Şti. (bundan sonra "Sarıkaya Net" olarak anılacaktır) bünyesinde işlenen, saklanan ve iletilen tüm bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkeleri çerçevesinde korunmasını sağlamaktır. Bu doğrultuda firma; ISO/IEC 27001:2022 standardına ve BTK Şebeke ve Bilgi Güvenliği Yönetmeliği gereksinimlerine uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmayı, işletmeyi, sürekli izlemeyi ve iyileştirmeyi taahhüt eder.

Politikanın spesifik hedefleri şunlardır:

- Abonelere ait kişisel veriler ile haberleşme içeriğinin yetkisiz erişime karşı korunması (gizlilik).
- Faturalama, abonelik ve şebeke yönetim verilerinin doğruluğunun ve tamlığının güvence altına alınması (bütünlük).
- İnternet erişim hizmetinin ve destek sistemlerinin kesintisiz sunulması (erişilebilirlik).
- Yasal ve düzenleyici yükümlülüklere (KVKK, 5651, 5809, BTK Yön.) tam uyumun sağlanması.
- Bilgi güvenliği farkındalığının kurum kültürüne yerleştirilmesi ve sürekli iyileştirme (PUKÖ) döngüsünün işletilmesi.

2. Kapsam

Sarıkaya Net, Denizli ili Pamukkale ilçesinde merkez ofisi üzerinden İnternet Servis Sağlayıcılığı (B Tipi) faaliyeti yürüten bir internet servis sağlayıcısıdır. Firma, toplam 3514 aboneye (3380 bireysel, 134 kurumsal) hizmet vermektedir. Bu politika ve BGYS kapsamı aşağıdaki unsurları içerir:

2.1. Kapsam Dahilindeki Varlıklar

- Abone kişisel verileri, sözleşmeler ve faturalama bilgileri.
- Şebeke altyapısı: Mikrotik (router ve switch) ağ ekipmanları, POP lokasyonları ve CGNAT altyapısı.
- Sunucu altyapısı: 2 adet sunucu üzerinde çalışan VMware ESXi sanallaştırma ortamı; RADIUS, faturalama ve web API hizmetleri.
- Firma tarafından geliştirilen faturalama, müşteri yönetimi ve muhasebe yazılımları.
- 5651 sayılı Kanun kapsamında tutulan internet erişim ve trafik kayıtları (loglar).
- Merkez ofis ve Türk Telekom binasındaki teknik ortamlar ile bu ortamlardaki fiziksel varlıklar.

Hazırlayan	Onaylayan
Bilgi Güvenliği Sorumlusu	Genel Müdür

2.2. Organizasyonel ve Coğrafi Sınırlar

BGYS kapsamı, firmanın tüm departmanlarını (Genel Müdürlük, Teknik, Muhasebe, Pazarlama) ve toplam 5 çalışanı ile firma adına görev yapan dış kaynaklı personeli kapsar. Coğrafi olarak merkez ofis, Türk Telekom binasındaki teknik alan ve şebeke kapsamındaki POP lokasyonları dahildir.

2.3. Hariç Tutmalar

Türk Telekom'un kendi sorumluluğundaki toptan altyapı bileşenleri (santral içi pasif altyapı vb.) ile dış kaynaklı hizmet sağlayıcıların kendi iç süreçleri, ilgili tedarikçilerin sorumluluğundadır; firma bu ilişkileri SRK-PRO-009 Tedarikçi İlişkileri Prosedürü ile yönetir.

Tanımlar ve Kısaltmalar

Bu dokümanda geçen temel terim ve kısaltmalar aşağıda açıklanmıştır:

Terim / Kısaltma	Açıklama
BGYS	Bilgi Güvenliği Yönetim Sistemi (ISO/IEC 27001:2022).
Gizlilik	Bilginin yalnızca yetkili kişilerce erişilebilir olması.
Bütünlük	Bilginin doğruluğunun ve tamlığının korunması.
Erişilebilirlik	Bilginin yetkili kullanıcılarca ihtiyaç anında erişilebilir olması.
Bilgi Varlığı	Firma için değer taşıyan her türlü veri, sistem, yazılım, donanım ve hizmet.
ISS	İnternet Servis Sağlayıcı.
POP	Point of Presence — hizmet sunulan şebeke erişim/dağıtım noktası.
Log	Sistem ve şebeke olaylarının zaman damgalı kayıtları.
PUKÖ	Planla-Uygula-Kontrol Et-Önlem Al sürekli iyileştirme döngüsü.
İlgili Taraf	Firma faaliyetlerinden etkilenen veya etkileyebilen kişi/kurum.

3. Üst Yönetim Taahhüdü ve Liderlik

Sarıkaya Net üst yönetimi, bilgi güvenliğini stratejik bir öncelik olarak benimser ve aşağıdaki hususları taahhüt eder:

- BGYS'nin kurulması, işletilmesi ve sürekli iyileştirilmesi için gerekli insan kaynağı, bütçe ve teknik kaynakların tahsis edilmesi.
- Bilgi güvenliği hedeflerinin belirlenmesi ve firma stratejisi ile uyumlu hale getirilmesi (Bkz. SRK-PLN-001).
- Rollerin ve sorumlulukların açıkça atanması (Bkz. SRK-ATM-001, SRK-ATM-002).
- Yönetimin gözden geçirmesi toplantılarının düzenli yapılması (Bkz. SRK-PRO-014).

Genel Müdür Kamil Kabukçu, bu politikanın nihai sahibi ve onay merciidir.

Hazırlayan	Onaylayan
Bilgi Güvenliği Sorumlusu	Genel Müdür

4. Bilgi Güvenliği İlkeleri ve Beyanları

4.1. Gizlilik

Firma, abonelere ait kişisel verilerin ve haberleşme içeriğinin yalnızca yetkili kişilerce, görev gereği ve yetki sınırları dahilinde erişilebilir olmasını sağlar. Haberleşmenin gizliliği 5809 sayılı Kanun ve Anayasa'nın 22. maddesi güvencesindedir. Erişim kontrolleri SRK-PRO-005 ile yönetilir.

4.2. Bütünlük

Bilginin yetkisiz veya kazara değiştirilmesi önlenir. Firma tarafından geliştirilen yazılımların ve veritabanlarının bütünlüğü; değişiklik kontrolü (SRK-PRO-016), yedekleme (SRK-PRO-011) ve kriptografik kontroller (SRK-POL-006) ile korunur.

4.3. Erişilebilirlik

İnternet erişim hizmetinin ve destek sistemlerinin sürekliliği esastır. Firma, hizmet sürekliliği hedeflerini (RTO/RPO) belirler ve iş sürekliliği planları ile destekler (SRK-PRO-011). Mevcut durumda yedek hat bulunmadığından, bu husus bir risk olarak izlenmekte ve telafi edici tedbirler değerlendirilmektedir (Bkz. SRK-RPR-001).

5. Risk Yönetimi Yaklaşımı

Firma, bilgi güvenliği risklerini sistematik bir yöntemle yönetir. Varlıklar envanterlenir (SRK-LST-001), tehdit ve açıklıklar değerlendirilerek risk seviyeleri belirlenir ve kabul edilemez riskler için işleme planları oluşturulur. Risk değerlendirme metodolojisi SRK-PRO-003 Risk Değerlendirme ve İşleme Prosedürü'nde, sonuçlar ise SRK-RPR-001 Risk Değerlendirme Raporu'nda tanımlanır.

6. Roller ve Sorumluluklar

Rol	Bilgi Güvenliği Sorumluluğu
Genel Müdür	Politikayı onaylar, kaynak sağlar, yönetimin gözden geçirmesini yürütür, nihai sorumludur.
Bilgi Güvenliği Sorumlusu	BGYS'yi kurar ve işletir; iç tetkik, risk yönetimi ve olay yönetimini koordine eder.
Bilgi Güvenliği Komitesi	Riskleri ve kontrolleri gözden geçirir, kararları onaylar, YGG'ye katılır.
Teknik Personel	Şebeke, sunucu ve yazılım güvenliği kontrollerini uygular ve izler.
Tüm Çalışanlar	Politika ve prosedürlere uyar; güvenlik olaylarını ve zafiyetleri raporlar.
Dış Kaynaklı Personel	Sözleşme ve gizlilik taahhütlerine uyar; firma kontrollerine tabidir.

7. Bilgi Güvenliği Eğitimi ve Farkındalık

Hazırlayan	Onaylayan
Bilgi Güvenliği Sorumlusu	Genel Müdür

Tüm çalışanlara, işe başlangıçta ve düzenli aralıklarla bilgi güvenliği ve KVKK farkındalık eğitimi verilir. BTK Şebeke ve Bilgi Güvenliği Yönetmeliği m.16 uyarınca eğitimler en az iki yılda bir tekrarlanır ve kayıtları en az üç yıl saklanır. Eğitim programı SRK-PRO-015 ile yönetilir.

İlgili Mevzuat ve Standartlar

Bu politika aşağıdaki standart ve yasal düzenlemeler dikkate alınarak hazırlanmıştır:

- ISO/IEC 27001:2022 — Bilgi Güvenliği Yönetim Sistemleri
- ISO/IEC 27002:2022 — Bilgi güvenliği kontrolleri uygulama rehberi
- 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun
- 5809 sayılı Elektronik Haberleşme Kanunu
- BTK Şebeke ve Bilgi Güvenliği Yönetmeliği
- 5237 sayılı Türk Ceza Kanunu (m.132-140 özel hayatın gizliliği)
- Anayasa m.20, m.22 (özel hayat ve haberleşme gizliliği)

Gözden Geçirme ve Güncelleme

Bu politika, en az yılda bir kez veya bilgi güvenliğini etkileyen önemli bir değişiklik (yeni tehdit, mevzuat değişikliği, organizasyon değişikliği, ciddi güvenlik olayı) meydana geldiğinde Bilgi Güvenliği Sorumlusu tarafından gözden geçirilir. Gözden geçirme sonuçları yönetimin gözden geçirmesi toplantısına girdi olarak sunulur.

Politikada yapılan her değişiklik, revizyon tarihçesi tablosuna işlenir ve güncel sürüm tüm ilgili taraflara duyurulur. Eski sürümler SRK-PRO-001 Doküman Yönetim Prosedürü kapsamında arşivlenir.

Yürürlük ve Onay

Bu politika, Kamil Kabukçu (Genel Müdür) tarafından onaylandığı tarihte yürürlüğe girer. Politikaya uyum tüm çalışanlar ve dış kaynaklı personel için zorunludur. Politikanın ihlali, SRK-PRO-010 Bilgi Güvenliği Olay Yönetimi Prosedürü ve ilgili disiplin süreçleri kapsamında değerlendirilir.

Hazırlayan	Onaylayan
Bilgi Güvenliği Sorumlusu	Genel Müdür