BİLGİ GÜVENLİĞİ POLİTİKAMIZ

Bilgi Güvenliği Politikası, ARY Holding ve bağlı kurumlarda uygulanmak üzere, ARY Holding yönetimi tarafından oluşturulmuştur. Bu politikanın uygulanması ile ARY Holding yönetimi, Bilgi Güvenliği Yönetim Sistemi kapsamındaki hizmetlerinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin gerekleri olan aşağıdaki temel ilkeleri yerine getirmek için gerekli kaynakların ve prosedürlerin sağlanmasını taahhüt ve beyan eder.

Bilgi güvenliği politikası, yalnızca IT departmanının değil, ARY Holding ve bağlı kurumlarda görev yapan tüm çalışanların sorumluluğundadır. Her çalışan, BGYS kapsamında belirlenen prosedürleri uygulayarak kurumun bilgi varlıklarını korumakla yükümlüdür.

a) Kapsam dâhilinde tüm bilgi varlıklarının bilerek veya bilmeyerek yetkisiz kullanımı, değiştirilmesi, açıklanması ve hasara uğratılması önlenecektir.
b) BGYS (Bilgi Güvenliği Yönetim Sistemi) kapsamındaki hizmetleriyle ilgili olarak müşterilerden alınacak bilgilerin güvenli, doğru ve tam olması sağlanacaktır.
c) Müşterilerine ait iş maksadıyla toplanan bilgiler sadece bu maksatla kullanılacak ve hiçbir şekilde üçüncü şahıslarla paylaşmayacaktır.
d) Müşterilerine ilişkin iş gereksinimlerini yasal mevzuat gerekliliklerine uygun alt yapı, süreç ve personel ile yapılması için gerekli kaynaklar sağlanacaktır.
e) ARY Holding ve bağlı kurumlarda, kurumsal ve kişisel bilgilerin ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır. Bu kapsamda faaliyet gösterilen ülkelerin bağlı bulundukları kanun ve yönetmeliklerine uyumlu bir şekilde, kişisel veriler ve gizlilik tasnifi yapılmış verileri gerekli teknik ve idari tedbirlerin alınarak işlenmesi ve saklanması konusunda taviz verilemez.
f) "Bilmesi gereken" prensibine uygun erişim kontrolü sağlanacak ve bilgi yetkisiz erişime karşı korunacaktır.
g) BGYS'nin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeylere indirilecektir.
h) Bilgi; bilginin elektronik iletişimi, üçüncü taraflarla paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak her durumda korunacaktır.
i) Bilgi varlıkları, gizlilik dereceleri ile tanımlanacak ve çalışanlar tarafından uygulanması ile gizliliği ve bütünlüğü sağlanacaktır.
j) ARY Holding ve bağlı şirketleri, ülke mevzuatında yer alan yasa, yönetmelik, genelge ve sözleşmelerde belirtilen tüm gerekliliklere uygun hareket edecektir.
k) Müşterilere sağlanan hizmetler iş süreçlerini büyük felaketlerin ve işletim hatalarının etkilerinden korumak amacıyla, iş sürekliliği yönetimi uygulanacak ve iş sürekliliği yönetim planı oluşturulacaktır. İş sürekliliği planının sürekliliği sağlanacak ve test edilecektir.
l) Personelin bilgi güvenliği farkındalığını arttıracak ve sistemin işleyişine katkıda bulunmasını teşvik edecek eğitimler düzenli olarak kurum çalışanlarına ve yeni işe giren çalışanlara sağlanacaktır. Eğitim zorunludur.
m) Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlâlleri rapor edilecek; tekrar etmesini engelleyici önlemler alınacaktır.

n) Personelin çalışma alanlarında, "Temiz Ekran / Temiz Masa" prensiplerine uygun olarak, "*Tasnif Dışı*" özellikteki bilgiler dışında bilgilerin, başkalarınca görülmesine imkân verilmeyecek şekilde önlemler alınacaktır.

o) ARY Holding, BGYS'nin uygulanması için çatı standart olarak ISO 27001 :2022 BGYS standardını, teknik olarak ISO 27002:2022 (BGYS) Uygulama Prensipleri tekniklerine uyum sağlamayı hedeflemektedir. ARY Holding, BGYS' ye ek olarak ISO 27701 :2025 (KVYS) kılavuzunu da kişisel veri koruma için uygulamayı hedeflemektedir.

p) ARY Holding'in mevcut stratejik iş planı ve risk yönetimi çerçevesi, BGYS'nin kurulup sürekliliğinin sağlanması için ilgili riskleri belirlemek, tanımlamak, değerlendirmek ve kontrol etmek işlevini yerine getirmektedir.

q) Risk değerlendirme, uygulanabilirlik bildirimi ve risk müdahale planı, bilgi ile ilgili risklerin nasıl kontrol edildiğini açıklamaktadır. Bilgi Güvenliği Yöneticisi ve Bilgi Sistemleri Yöneticisi, risk müdahale planının yönetiminden ve idamesinden sorumludur. Ek risk değerlendirmeleri, gerekli olduğu takdirde, belirli riskler için uygun kontroller belirlemek amacıyla yürütülebilir.

r) Özellikle, iş sürekliliği ve acil durum planları, veri yedekleme işletme dokümanları, virüslerden ve bilgisayar korsanlarından sakınma, erişim kontrol sistemleri ve bilgi güvenliği ihlal bildirimi, bu politika için esastır.

Tüm ARY Holding ve bağlı kurum çalışanlarının ve BGYS'nde tanımlanan belirli kurum dışı tarafların bu politikaya ve bu politikayı uygulayan BGYS' ye uymaları beklenmektedir. Tüm personel ve belirli şirket dışı taraflar, uygun eğitimi alacaklardır.

BGYS, sürekli ve sistematik değerlendirme ve geliştirmeye tabidir.

ARY Holding, BGYS çerçevesini desteklemek ve güvenlik politikasını periyodik olarak gözden geçirmek amacıyla, ARY Holding yönetimi tarafından yönetilen ve Bilgi Güvenliği Yöneticisi ile diğer yöneticilerin dahil olduğu bir bilgi güvenlik komitesi oluşturmuştur.

Bu politika, risk değerlendirmede veya risk müdahale planındaki değişikliklere yanıt vermek amacıyla yılda en az bir kez gözden geçirilecektir.

ONAYLAYAN YETKİLİLER

Hazırlayan	Kontrolör	Onaylayan	Onaylayan
Sefa SAKARYA	Bahadır KARA	Bülent GÜNEY	Ercüment TÜRKER
BT Yönetişim Kıdemli Uzmanı	BT Yönetişim Müdürü	CIO	COO

Herkese Açık