
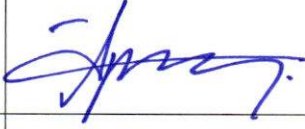





BİLGİ GÜVENLİĞİ POLİTİKASI

DOKÜMAN NUMARASI	PO.01	
REVİZYON NUMARASI	02	
REVİZYON TARİHİ	12.04.2023	
YAYIN TARİHİ	03.07.2019	
KONTROL KRİTERİ	Md. 5.2	
TASNİF	Tasnif Dışı	
HAZIRLAYAN	Yurdagül KELEŞ	
KONTROL EDEN	Rahmi Alpay ÖZPINAR	
ONAYLAYAN	Haluk Recai BOSTAN	

DEĞİŞİKLİK TAKİP LİSTESİ

No	Tarih	Açıklama
00	03.07.2019	İlk Yayın
01	17.03.2020	Revizyon – 1: Rekabet Kurumunun asli görevi uygulama başlığına eklendi.
02	12.04.2023	Revizyon – 2: “Uygulama” bölümündeki politikalara bir madde eklendi; bir maddede revizyon yapıldı.

İÇİNDEKİLER

1. AMAÇ.....	2
2. KAPSAM	2
3. SORUMLULUKLAR	2
4. UYGULAMA	2
5. TANIMLAR.....	3

1. AMAÇ

Bilgi Güvenliği Yönetim Sisteminin amacı; bilginin “gizlilik”, “bütünlük” ve “erişilebilirlik” kapsamında değerlendirilerek içeriden ve/veya dışarıdan gelebilecek, kasıtlı veya kazayla oluşabilecek tüm tehditlerden uygun şekilde korunmasını ve yürütülen faaliyetlerin güvenli olarak gerçekleştirilmesini temin etmektir.

Bilgi güvenliği politikasının amacı ise, BGYS kapsamında temel bilgi güvenliği prensiplerinin tanımlanması, tüm ilgili taraflara Rekabet Kurumu’nun bilgi güvenliği gereksinimlerinin bildirilmesi ve uyulması istenen kuralların yazılı temel dayanağının oluşturulmasıdır.

2. KAPSAM

Bilişim Teknolojileri Dairesi Başkanlığı.

3. SORUMLULUKLAR

Yönetim Temsilcisi bu dokümanın güncellenmesinden sorumludur.

4. UYGULAMA

Bilişim Teknolojileri Dairesi Başkanlığının Bilgi Güvenliği Politikası, Daire Başkanlığı tarafından yürütülen faaliyetlerde ve Rekabet Kurumunun misyonu olan, "Rekabet ortamının sağlanması, korunması ve geliştirilmesi amacıyla mal ve hizmet piyasalarındaki rekabeti engelleyici, bozucu veya kısıtlayıcı anlaşma, karar ve uygulamalar ile piyasaya hâkim olan teşebbüslerin bu hâkimiyetlerini kötüye kullanmalarını önlemek, bunun için gerekli düzenleme ve denetlemeleri yaparak rekabetin korunmasını sağlamak” faaliyetlerinde bilgi güvenliğini sağlamak için,

- Bilgi Güvenliğinin üç temel ögesi olan “Gizlilik, Bütünlük ve Erişilebilirliği” sağlamak,
- Bilgi varlıklarını yönetmek, bilgi ve bilgi işlem olanaklarının ihtiyaçlarını ve risklerini belirlemek, risklere yönelik kontrolleri geliştirmek ve uygulamak, risklerin işlenmesi için çalışma esaslarını ortaya koymak, riskleri yönetmek,
- İş sürekliliğine yönelik tehditlerinin etkisini azaltmak ve iş sürekliliğine katkıda bulunmak.
- Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmak,
- Yasal mevzuat ve düzenleyici yapıların şartlarına uyumu sağlamak,

- Karşılıklı sözleşme, protokol ve benzeri anlaşmaların içerdiği yükümlülüklere uyumu temin etmek,
- BGYS özelinde hedefler belirlemek ve belirli dönemlerde uygunluklarını değerlendirerek, BGYS kapsamında risk yönetimini gerçekleştirmek,
- BGYS'nin sürekli iyileştirilmesini taahhüt etmek; bu çerçevede bilgi güvenliği amaç ve hedeflerini belirleyerek, belirli aralıklarla "Yönetim Gözden Geçirme Toplantıları" gerçekleştirerek ve BGYS'nin uygulanmasını takip ederek sistemin sürdürülebilirliğini sağlamaktır.

Bilgi güvenliği politikası tüm çalışanlara iletilir. Uygulanabilir durumlarda ilgili taraflarla paylaşılır. Yılda en az bir kez veya büyük bir değişiklikte derhal gözden geçirilir.

5. TANIMLAR

BGYS : Bilgi Güvenliği Yönetim Sistemi.

Gizlilik : Bilgiye erişimin, sadece yetkisi bulunan kişiler ile kısıtlı kalması.

Bütünlük : Bilginin, yetkisiz kişilerce veya yanlışlıkla değiştirilmesi, silinmesi ya da her hangi bir şekilde tahribine karşı korunması.

Erişilebilirlik: Bilginin ihtiyaç duyulduğu her an kullanıma hazır olması.