

Bilgi Güvenliđi Genel Politikası

Garanti Faktoring A.Ş.
Organizasyon ve Süreç Gelişim Birimi

İstanbul, Temmuz 2026

No.: OSGMBGPO0002_22 Versiyon no.: 10 Tarih: 22/07/2026

Bir sonraki gözden geçirme tarihi: 22/07/2027

Düzenleyen Birim: Organizasyon ve Süreç Gelişim

Uygulama Kapsamı: Garanti Faktoring A.Ş.

Sorumlu: Yönetim Kurulu

Etiket(ler): Politika

Bilgi Güvenliđi Genel Politikası

İçerik

1. Giriş	4
2. Uygulama Amacı ve Kapsamı.....	4
3. Genel İlkeler	5
4. Kılavuz İlkeler	5
5. Sorumluluk ve İhlal	7
6. Süreçle İlgili Kontroller	7
7. Referanslar / İlgili Dokümanlar	9
8. Onay, Gözden Geçirme ve Denetim Hükümleri	9
SÖZLÜK	10
9. Deđişikliklere İlişkin Açıklama	11

1. Giriş

Garanti Faktoring A.Ş. üst yönetimi, bilgi ve bilgi varlıklarını koruyacak yapıları kurmak ve güvenlik önlemlerinin uygun düzeye getirilmesi amacıyla ilgili politikaları belirler, çalışmaları yönlendirir ve destekler. Bilgi Güvenliği politikası bu bağlamda oluşturulmuştur ve Garanti Faktoring A.Ş.'nin tabi olduğu her türlü ulusal ve uluslararası yasa, mevzuat ve düzenlemelere uyumu destekler

2. Uygulama Amacı ve Kapsamı

Amaç

Bilgi Güvenliği Politikası'nın amacı, Banka ve Garanti BBVA Teknoloji Merkezi ilgili Kurumsal Güvenlik birimleri koordinasyonunda, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına ve bu standardı destekleyen diğer standartlara uygun olarak yürütülmesini sağlamak , Firma genelinde uygulanacak temel bilgi güvenliği prensiplerini belirlemek ve Garanti Faktoring A.Ş. Yönetim Kurulu'nun söz konusu prensiplere verdiği desteği ifade etmektir. Firma'da, Banka ve Garanti BBVA Teknoloji Merkezi ilgili Kurumsal Güvenlik birimleri koordinasyonu ile uygulanmakta olan Bilgi Güvenliği Yönetim Sistemi'nin amaç ve hedefleri aşağıda listelenmiştir.

- Firmanın tabi olduğu her türlü ulusal ve uluslararası yasa, mevzuat ve düzenlemeler ile sözleşmeler gibi ilgili taraflardan doğan yükümlülüklerinin yerine getirilmesi,
- Firma'nın maruz kalabileceği her türlü iç ve dış siber tehditlere karşı önleyici tedbirlerin alınması ve olası vakaların en az etki ile atlatılmasına yönelik hazırlıkların yapılması,
- Firmanın kritik süreçlerine dair iş sürekliliği planlarının oluşturulması ve işletilmesinde bilgi güvenliği hususlarının göz önünde bulundurulması,
- Firmanın, müşterilerinin, iş ortaklarının ticari sırlarının, itibarının ve bilgilerinin korunması,
- Firma çalışanlarının ve müşterilerinin kişisel bilgilerinin korunması,
- Firma'nın, iş süreçlerinin en az yetki prensibine uygun olarak işletilmesi,
- Firma içinde teknik ve teknik olmayan projelerle ilgili bilginin korunması ve gerektiğinde bilgi birikiminin erişilebilir olması,
- Bilgi güvenliği bilincinin kurum kültürünün bir parçası haline getirilmesi ve çalışanların farkındalık düzeylerinin sürekli yüksek tutulması,

- Üçüncü taraflar ile yapılan sözleşmelerin bilgi güvenliğini gözeterek şekilde yapılması

Uygulama Kapsamı

Garanti Faktoring A.Ş. stratejik hedeflerinin desteklenmesi, marka değerinin korunması, yasal düzenlemelere uyum, BT risklerinin yönetimi ve değişen siber tehditlere yanıt verebilmek amacıyla gerekli bilgi güvenliği kuralları ve prensipleri Bilgi Güvenliği Politikası kapsamındadır.

Garanti Faktoring A.Ş. mülkiyetinde olan her türlü bilgi varlığı Bilgi Güvenliği Politikası kapsamında olup tüm iş süreçleri Bilgi Güvenliği Politikasına uygun olarak yürütülür.

3. Genel İlkeler

3.1. Firma faaliyetlerinde kullanılmak üzere oluşturulan bu politika aşağıdaki prensipleri göz önünde bulundurur

- Erişilebilirlik
- Bütünlük
- Gizlilik
- Şeffaflık
- Farkındalık
- Risk yönetimi
- Mevzuatlara daimi uyum

4. Kılavuz İlkeler

Kılavuz İlkeler başlığı altında aşağıda tanımlanan ilke ve süreçler, Banka ve Garanti BBVA Teknoloji Merkezi koordinasyonunda uygulanır.

4.1 Firma iş süreçlerinin tasarım ve işletilmesinde, söz konusu süreçlerin bilgi güvenliği gereksinimlerinin belirlenmesi ve belirlenen gereksinimlerin karşılanması amacıyla etkin yöntemlerin uygulanması esastır. İş süreçlerinin zaman içinde değişen çevresel etkilere veya değişen bilgi güvenliği gereksinimlerine göre güncellenmesi, iş süreci sahibinin sorumluluğundadır.

4.2 Firma mülkiyetinde olan her türlü bilgi / bilgi varlığını hedef alan tehditlere karşı gerekli tespit ve engelleme yöntemleri hayata geçirilir. Söz konusu yöntemlerin güncel tehditlere karşı etkin koruma sağlamasını temin

eden test ve iyileştirme faaliyetleri yürütülür. Bu kapsamda gerekli yatırım, proje ve insan kaynağı ihtiyaçları planlanarak hayata geçirilir.

4.3 Bilgi varlıklarının taşıdığı bilgi güvenliği risklerinin tamamen yok edilmesinin mümkün olmadığı ve her durumda “artık risk” olacağı bilinci ile mevcut risklerin yönetilmesi, söz konusu artık riski en aza indirecek düzeltici ve önleyici kontrollerin etkin şekilde uygulanması esastır. Bu kapsamda olan çalışmalar ilgili Risk Yönetimi Politikalarına uygun olarak yürütülür.

4.4 Firma iş süreçleri tasarımında ve işletiminde bilinen bilgi güvenliği riskleri değerlendirilerek kabul edilenler dışındaki risklerin olasılıklarını ve/veya etkilerini azaltıcı bilgi güvenliği kontrolleri oluşturulur. Risk değerlendirme faaliyetinin ve kontrollerin etkin biçimde işletilmesi Garanti BBVA Teknoloji Merkezi ilgili birimleri ve iş süreci sahibi sorumluluğundadır.

4.5 Firma bünyesinde üretilen, işlenen, saklanan veya iletilen her türlü bilgi ve bilgi varlığı Firma mülkiyetindedir. Bilgi ve bilgi varlıklarının güvenlik ihtiyaçlarının gerektirdiği şekilde sınıflandırılması, belirlenen sınıfa uygun olarak koruma yöntemlerinin belirlenmesi ve işletilmesi bilgi / bilgi varlığı sahibinin sorumluluğundadır.

4.6 Bilgi güvenliği kapsamında yürütülen faaliyetlerin hedeflenen başarıya ulaşabilmesi için kullanıcıların konuya bilinçli yaklaşımı ve sorumluluk alanlarına düşen görevleri yerine getirmesi, yayınlanan politika, standart, prosedür, kılavuz ve duyurulara azami derecede özen göstermesi esastır. Bu kapsamda; Firma, çalışanlarının bilgi güvenliği farkındalığını arttırmak ve bu farkındalığın Firma kültürünün bir parçası haline getirmek amacıyla çalışmalar yürütülür.

4.7 Firma mülkiyetinde olan bilgi veya bilgi varlıklarına erişimler kullanıcıların rol ve sorumluluklarıyla uyumlu şekilde sınırlandırılır. Söz konusu sınırlandırma yöntemlerinde kullanılacak doğrulama ve yetkilendirme yöntem ve mekanizmalarının belirlenmesi, güncellenmesi ve denetim amaçlı iz kayıtlarının güvenli olarak saklanması amacıyla gerekli altyapılar tesis edilir.

4.8 Firma mülkiyetinde olan bilgiyi ve bilgi varlıklarını hedef alan siber saldırılar bilgi güvenliği olay yönetimi kapsamında değerlendirilir. Yapılan değerlendirmeler neticesinde, mevcut kontrollerin güncellenmesi veya yeni kontrollerin devreye alınması faaliyetleri en kısa zamanda gerçekleştirilir. Söz konusu faaliyetler Türkiye Garanti Bankası A.Ş. Siber Güvenlik Politikası'na uygun olarak yürütülür.

4.9 Firma bilgi varlıkları belirlenerek, bu varlıklar üzerinde oluşabilecek potansiyel tehdit ve zafiyetler analiz edilir. Bu potansiyel tehdit ve zafiyetlerin etkilerini azaltmak için gerekli çalışmalar Risk Yönetimi süreçleri kapsamında yürütülür. Bilgi güvenliğini sağlamak amacıyla bilgi varlıklarının kullanımı kayıt altına alınır ve bu kayıtlar istatistik ve denetim amacıyla kullanılabilir.

4.10 Üçüncü taraflarla yapılacak çalışmalar öncesinde ilgili taraflar Firma bilgi güvenliği kuralları ve prensipleri hususunda merkezi satın alma süreçleri kapsamında ilgili taahhütnameler ve sözleşmede yer alacak maddeler aracılığıyla bilgilendirilir. İlgili Firma ilgili bölümü sorumluluğunda gerekli

maddeler sözleşmeye eklenir ve gerekli görüldüğü durumda Gizlilik Taahhütnamesi ilgililere imzalatılır.

4.11 Bu politikada yer alan amaç ve hedefleri destekleyen çalışmalar, her yıl Banka ve Garanti BBVA Teknoloji Merkezi ilgili Güvenlik birimleri tarafından yürütülen “Bilgi Güvenliği Yönetim Sistemi” kapsamında, Banka Bilgi Güvenliği Politikası çerçevesinde uygulanır ve bu çalışmaların ilerleme durumları, ilgili birimler ile koordineli olarak yürütülür.

4.12 BGYS’nin sürekli iyileştirilmesine yönelik çalışmalar ilgili komiteler tarafından düzenli olarak gözden geçirilir, kaynak gereksinimleri belirlenir, önceliklendirilerek temin edilir, çeyrek dönemler halinde iştirak Bilgi Güvenliği Yönetim Sistemleri bilgilendirmeleri yapılır.

4.13 Bilgi Güvenliği Politikası çerçevesinde belirli kapsamlar dahilinde yardımcı politikalar ve prosedürler yayınlanır

5. Sorumluluk ve İhlal

Garanti Faktoring A.Ş. çalışanları, Bilgi Güvenliği Politikası ve diğer destekleyici dokümanlara uygun davranmakla yükümlüdür.

Tüm yöneticiler, yönetici oldukları bölüm / birimlerde politikanın uygulanmasından, çalışanlarının bilgi sistemlerine ilişkin güvenlik politikalarına uymasından doğrudan sorumludur.

Yukarıda belirtilen politikalara uymayan kullanıcılar hakkında iç disiplin süreçleri işletilir, gerek olması halinde disiplin kararı alınabilir ve/veya söz konusu çalışanın iş akdi, İş Kanunu’na göre tek taraflı haklı nedenle fesh edilebilir.

6. Süreçle İlgili Kontroller

No	Kontrol	Kontrol Sahibi	Kontrol Eden
1	Organizasyon ve Süreç Gelişimi birimi, Bilgi Sistemleri üzerinde edinilen, saklanan, iletilen, işlenen verileri güvenlik hassasiyet derecelerine göre sınıflandırılmasını sağlar.	Garanti Faktoring	Organizasyon ve Süreç Gelişimi birimi
2	Garanti BBVA Teknoloji Merkezi, Bilgi Sistemleri	Garanti BBVA Teknoloji Merkezi	Organizasyon ve Süreç Gelişimi birimi

No	Kontrol	Kontrol Sahibi	Kontrol Eden
	üzerinde edinilen, saklanan, iletilen, işlenen verileri güvenlik hassasiyet derecelerine göre sınıflandırılmasını temin eder.		
3	Garanti BBVA Teknoloji Merkezi, Garanti Faktoring özelinde gerçekleşen yetkisiz erişim teşebbüsleri ve bilgi güvenliği ihlallerini ilgili birimlere / İç Kontrol ve Uyum birimine raporlanmasını sağlar.	Garanti BBVA Teknoloji Merkezi	İç Kontrol ve Uyum (Uygulama Seviyesi) GT-1. Seviye Operasyonel Risk ve Kontrol (Veri tabanı ve İşletim Sistemi)
4	Organizasyon ve Süreç Gelişimi birimi, bilgi güvenliği hususunda personelin farkındalığını arttıracak bilgilendirme veya çalışmaların Garanti BBVA Teknoloji Merkezi tarafından yapıldığını takip eder.	Garanti Faktoring	Organizasyon ve Süreç Gelişimi birimi
5	Organizasyon ve Süreç Gelişimi birimi, dışarıdan gelecek bir siber saldırıya karşı gerekli önlemlerin alındığını kontrol etmek amacıyla 2 yılda bir Garanti BBVA Teknoloji Merkezi tarafından sızma testi yaptırılıp yaptırılmadığını takip eder.	Garanti Faktoring	Organizasyon ve Süreç Gelişimi birimi
6	İç kontrol ve Uyum birimi yılda bir kez yönetim kuruluna sunulmak üzere; yetkisiz erişim teşebbüslerini, bilgi güvenliği sürecine uyum durumunu, bilgi güvenliği ihlaline ilişkin olayları içeren güvenlik ihlalleri raporu hazırlar. Rapora Garanti Faktoring kurum	Garanti BBVA Teknoloji Merkezi	İç Kontrol ve Uyum Birimi

No	Kontrol	Kontrol Sahibi	Kontrol Eden
	içerisinde yaşanan güvenlik ihlalleri de güvenlik ihlalleri raporuna dahil edilerek üst yönetime sunulur.		

7. Referanslar / İlgili Dokümanlar

- Veri Güvenliği Prosedürü
- İş Sürekliliği Politikası
- Risk Yönetimi Politikası
- Türkiye Garanti Bankası A.Ş. Siber Güvenlik Politikası
- Türkiye Garanti Bankası A.Ş. Bilgi Güvenliği Politikası
- Türkiye Garanti Bankası A.Ş. Finansal Olmayan Risk Yönetimi Politikası

8. Onay, Gözden Geçirme ve Denetim Hükümleri

- 5.1. Bu politika, "Yönetim Kurulu" tarafından 22/07/2026 tarihinde onaylanmış ve 22/07/2027 tarihinde 1 yıl süresince geçerli olmak üzere yürürlüğe alınmıştır.
- 5.2. İşbu Politika, Organizasyon ve Süreç Gelişim birimi tarafından ve Garanti BBVA Teknoloji Merkezi işbirliği ile kendi sorumluluk alanları dahilinde hazırlanmıştır.
- 5.3. Bu politikanın firma bazında yürütülmesinden Organizasyon ve Süreç Gelişim birimi sorumludur. Bu itibarla, Politika'nın onaya sunulması, yayınlanması, Politikaya tabi kişilerin bu konudaki farkındalığının artırılmasından sorumlu olacaklardır.
- 5.4. Politikadan etkilenen alanlardan sorumlu Üst Düzey Yöneticiler, kendi sorumluluk alanları dahilinde ve uygulanabildiği ölçüde, Politikaya uyum için yeterli araçları, sistemleri ve yapıyı sağlayacaktır.
- 5.5. İşbu Politikaya uyum derecesi ve gelişimi yürürlükte olan kontrol modeline göre izlenecektir. Garanti Faktoring A.Ş.'de çeşitli kontrol fonksiyonları ve birimleri, kendilerine verilen yetki ve görevlere uygun olarak politikanın uygulamasının izlenmesinde aktif bir biçimde ve düzenli olarak işbirliği yapacaklardır.

- 5.6. Tespit edilen yönetim modeline uygun olarak, Genel Politikaların uygulaması, Garanti Faktoring A.Ş.'nin nihai denetleme ve yönetim organı olarak Şirketin Yönetim Kurulu, tarafından doğrudan doğruya ya da ilgili komiteleri aracılığıyla dolaylı olarak, Şirket İç Kontrol ve Uyum Birimi, veya uygulanabildiği ölçüde, Garanti BBVA nezdindeki iç denetim ve/veya kontrol fonksiyonları tarafından periyodik veya isteğe bağlı olarak düzenlenecek olan raporlarla izlenecek ve takip edilecektir.
- 5.7. Yılda en az bir defa veya ortaya çıkan gelişmeler ışığında gerektiği durumda Politika'nın revizyonu için Organizasyon ve Süreç Gelişim birimi tarafından gözden geçirme faaliyetleri gerçekleştirilecek ve gereken ya da arzu edilen değişiklikler Garanti Faktoring A.Ş. Yönetim Organlarına sunulacaktır.
- 5.8. Garanti Faktoring A.Ş. internet sitesinde yer alan Bilgi Güvenliği Politikası hakkındaki bilgiler Bilgi Güvenliği Politikası dokümanını referans alır ve gerekli güncelleme, gözden geçirme çalışmaları doküman versiyonu referans alınarak yürütülür.
- 5.9. Bu Politika'nın veya buna dair diğer İç Yönetmeliklerin hükümlerine uyulmaması, uygulama kapsamındaki çalışanlar ve üst düzey yöneticiler için disiplin yaptırımlarının uygulanmasına yol açabilir.
- 5.10. Sorumluluk alanı içinde olmasa dahi, işbu Politika ve veya ilgili İç Yönetmeliklere, değer ve ilkelere aykırı olabilecek bir eylem veya durum hakkında bilgiye, emareye veya şüpheye sahip olan kişilerin, Etik Bildirim Hattı dahil olmak üzere Etik ve Doğruluk İlkelerinde belirtilen adımlara uygun olarak bildirimde bulunmaları zorunludur.

SÖZLÜK

- Firma** : Garanti Faktoring A.Ş.
- Yönetim Organları** : Garanti Faktoring A.Ş. Yönetim Kurulu ya da ilgili komiteleri
- Banka** : Garanti Bankası T. A.Ş.
- Çalışan** : Garanti Faktoring A.Ş. çalışanıdır.
- Dış Kaynaklı Çalışan** : Garanti Faktoring A.Ş.' bir sözleşme kapsamında hizmet veren harici firmaya bağlı personel
- Stajyer** : Garanti Faktoring A.Ş.' ye hizmet veren tam veya yarı zamanlı stajyer çalışan
- Bilgi Varlığı (Bilgi Sistemleri)** : Garanti Faktoring A.Ş.' nin iş süreçlerinin işletiminde kullanılan her türlü bilgi, donanım, yazılım, hizmet, belge ve çalışanlardır.
- Bilgi Güvenliği** : Bilgi varlıkları için aşağıdaki özelliklerinin korunmasıdır.
- **Gizlilik:** Bilginin sadece yetkili kullanıcılar tarafından erişilebilir olması,

- **Bütünlük:** Bilginin yetkisiz kullanıcılar tarafından değiştirilmeden korunması ve değiştirildiğinde farkına varılması,
- **Erişilebilirlik:** Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması

Bilgi Güvenliği Yönetim Sistemi (BGYS) : Firma itibarının, müşteri mahremiyetinin ve bilgi varlıklarının güncel bilgi güvenliği tehditlerine karşı korunması amacıyla işletilen sistemdir.

HYS / SMART : Hizmet Yönetim Sistemi.

9. Değişikliklere İlişkin Açıklama

Versiyon	Tarih	Değişiklik Özeti	Değişikliği Yapan
V01	06/09/2012	İlk yazım	Nazan AKTAŞ
V02	19/08/2015	RM, KKB veri paylaşımı eklenmiştir	Nazan AKTAŞ
V03	12/10/2018	Gözden Geçirme	Nazan AKTAŞ
V04	03/06/2020	BDDK İlkeler Tebliğine Göre Güncelleme	Nazan AKTAŞ
V05	15/10/2021	Gözden geçirme ve 2, 3, 4, 5 ve 8 no'lu başlıklarda güncelleme yapılmıştır.	Nazan AKTAŞ
V06	25/07/2022	Gözden geçirme ve yeni şablon düzenleme	Nazan AKTAŞ
V07	25/07/2023	Gözden geçirme	Nazan AKTAŞ
V08	22/07/2024	Gözden geçirme	Nazan AKTAŞ
V09	22/07/2025	Garanti BBVA referans dokümanına göre güncelleme	Nazan AKTAŞ
V10	22/07/2026	Garanti BBVA referans dokümanına göre güncelleme	Nazan AKTAŞ