Bilgi Güvenliği Genel Politikası

Garanti Faktoring A.Ş.

Organizasyon ve Süreç Gelişim Birimi

İstanbul, Temmuz 2022

Bilgi Güvenliği Genel Politikası

İçerik

1. Giriş

2. Uygulama Amacı ve Kapsamı

Amaç
Garanti Faktoring A.Ş. üst yönetimi; bilgi varlıklarını koruyacak yapıları kurmakta ve güvenlik önlemlerinin uygun düzeye getirilmesi hususunda yürütülecek çalışmaları desteklemektedir.

Bu dokümanın amacı, Garanti Faktoring A.Ş. paydaşlarını bilgi güvenliği yönetim sistemi çerçevesi ve prensipleri hakkında bilgilendirmektir..

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. Bilgi Güvenliği Amaç ve Hedefleri

Garanti Faktoring A.Ş. (Firma) üst yönetimi; bilgi ve bilgi varlıklarını koruyacak yapıları kurmakta ve güvenlik önlemlerinin uygun düzeye getirilmesi hususunda yürütülecek çalışmaları desteklemektedir.

Firma, kendisine veya müşterilerine ait bütün bilgilerin ve bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğine yönelik iç veya dış, kasıtlı veya kasıtsız bütün tehditlere karşı korumak için gerekli teknik ve idari bilgi güvenliği önlemlerini almayı amaçlamaktadır.

Bu nedenle bilgi güvenliği yönetim sisteminin planlama, uygulama, izleme ve iyileştirme adımları belirlenen bölümler ve servisler için 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 yürütülür.

Firmada Banka ve Garanti BBVA Teknoloji Merkezi ilgili Kurumsal Güvenlik birimleri koordinasyonuyla 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 gözetecek şekilde yapılması. ,

3.2. Bilgi Güvenliği Yönetim Sistemi

- Tüm bilgi kaynakları ve onu destekleyen unsurlar politika ve prosedürlerde belirlenen yöntemler dahilinde korunmalıdır.
- Bilgi güvenliği, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ile temin edilmelidir.
- Yasal mevzuat ve diğer düzenleyici kurallar doğrultusunda bilgi varlıklarının ve müşteri sırlarının güvenliği "Veri Güvenliği Prosedürü"ne göre sağlanmalıdır.
- Başarılı bir güvenlik seviyesi için bu sorumlulukların bilinmesi ve uygulanması esastır. Bu sorumlulukların çalışan tarafından doğru anlaşılması için insan boyutunun çok iyi yönetilmesi, eğitim ve bilinçlendirme çalışmaları ile güçlendirilmesi gerekmektedir. Bu kapsamda Banka ve Garanti BBVA Teknoloji Merkezi ilgili Kurumsal

Güvenlik birimleri yönlendirmesiyle çalışanların bilgi güvenliği konusundaki farkındalığını arttıracak eğitimler ve faaliyetler düzenlenir.

- Tüm firma çalışanı, elektronik haberleşme ortamında (intranet) yayınlanan bilgi güvenliğine ilişkin politikalara, standart ve prosedürlere uymak zorundadır.
- Tüm firma çalışanı, işinin bir parçası olarak eğitimlerde ve bilgi güvenliği politika ve prosedürlerinde bahsedilen güvenlik kurallarını uygular ve çalıştığı bölümde kullanılmasını sağlar.
- Herhangi bir çalışanın bilinçli olarak güvenlik kurallarını ihlal veya ihmal etmesi durumunda firmanın disiplin süreci uygulanır.
- Çalışanlar bilişim kaynaklarında kendilerine tanımlanan şifrelerin, erişimlerin ve yetkilerin kullanımına, güvenliğine ve gizliliğine özen gösterir. Bu kullanımlar tamamıyla kişilerin kendi sorumluluğundadır.
- Çalışanlar, Bilgi Güvenliği Politikaları kapsamında gördükleri/tespit ettikleri ihlal olayları, zafiyet ve açıklıkları, HYS / Smart üzerinden "Güvenlik Vaka Yönetimi - Bilgi Güvenliği Vaka İnceleme" kategorisinden kayıt açarak, Garanti BBVA Teknoloji Merkezi - "Güvenlik Operasyonları Birimi - Vaka Yönetimi Bölümü" ne bildirir. Gerekli iletişimin sağlanması için Organizasyon ve Süreç Gelişim ekibine de maille bilgi verilir, gerekli durumlarda ilgili partilerle Vaka Yönetimi ekibince iletişim ve bilgi paylaşımı sağlanmaktadır.
- Firma bilgi varlıkları belirlenerek, bu varlıklar üzerinde oluşabilecek potansiyel tehdit ve zafiyetler analiz edilir. Analiz sonuçları aylık olarak Organizasyon ve Süreç Gelişim ve İç Kontrol ile paylaşılır. Bu potansiyel tehdit ve zafiyetlerin etkilerini azaltmak için gerekli çalışmalar Risk Yönetimi kapsamında yürütülür. Bilgi güvenliğini sağlamak amacıyla bilgi varlıklarının kullanımı kayıt altına alınır ve bu kayıtlar istatistik ve denetim amacıyla kullanılabilir.
- Bu politikada yer alan amaç ve hedefleri destekleyen çalışmalar, her yıl Banka ve Garanti BBVA Teknoloji Merkezi ilgili Kurumsal 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.
- Bilgi Güvenliği Yönetim Sisteminin sürekli iyileştirilmesi sağlanır, sürekli iyileştirmeye yönelik çalışmalar, yönetim tarafından gözden geçirilir.
- Bilgi Güvenliği Politikası çerçevesinde belirli kapsamlar dahilinde yardımcı politikalar ve prosedürler yayınlanır..

4. 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 üzerinde edinilen, saklanan, iletilen, işlenen verileri güvenlik hassasiyet derecelerine göre sınıflandırılmasını temin eder.	Garanti BBVA Teknoloji Merkezi	Organizasyon ve Süreç Gelişimi birimi
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	Garanti Faktoring	Organizasyon ve Süreç Gelişimi birimi

No	Kontrol	Kontrol Sahibi	Kontrol Eden
	testi yaptırılıp yaptırılmadığını takip eder.		
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 içerisinde yaşanan güvenlik ihlalleri de güvenlik ihlalleri raporuna dahil edilerek üst yönetime sunulur.	Garanti BBVA Teknoloji Merkezi	İç Kontrol ve Uyum Birimi

5. Referanslar / İlgili Dokümanlar

- Veri Güvenliği Prosedürü
- Türkiye Garanti Bankası A.Ş. Siber Güvenlik Politikası
- İş Sürekliliği Politikası

6. Onay, Gözden Geçirme ve Denetim Hükümleri

6.1. Bu politika, "Yönetim Kurulu" tarafından 25/07/2022 tarihinde onaylanmış ve 25/07/2023 tarihinde 1 yıl süresince geçerli olmak üzere yürürlüğe alınmıştır.

6.2. İşbu Politika, Organizasyon ve Süreç Gelişim birimi tarafından ve Garanti BBVA Teknoloji Merkezi işbirliği ile kendi sorumluluk alanları dahilinde hazırlanmıştır.

6.3. 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.

6.4. Politikadan etkilenen alanlardan sorumlu Üst Düzey Yöneticiler, kendi sorumluluk alanları dahilinde ve uygulanabildiği ölçüde, Politikaya uyum için yeterli araçları, sistemleri ve yapıyı sağlayacaktır.

6.5. 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.

6.6. Tespit edilen yönetişim 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.

6.7. 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.

6.8. Bu Politikanın veya buna dair diğer İç Yönetmeliklerin hükümlerine uyulmaması, uygulama kapsamındaki çalışanlar ve üst düzey yöneticiler için disiplin yaptırımlarının uygulanmasına yol açabilir.

6.9. Sorumluluk alanı içinde olmasa dahi, işbu Politikae 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 AŞ' bir sözleşme kapsamında hizmet veren harici firmaya bağlı personel

Stajyer : Garanti Faktoring AŞ' ye hizmet veren tam veya yarı zamanlı stajyer çalışan

Bilişim Kaynakları : Mülkiyet hakları Garanti Faktoring A.Ş.'ye ait olan, Firma tarafından lisanslanan/ kiralanan ya da kullanım hakkına sahip olunan her türlü ağ, sunucu, bilgisayar, donanım, yazılım ve servislerdir.

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.

7. 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