Viennalife Emeklilik ve Hayat A.Ş.

BGYS Politikası

Prosedür Künyesi	
Versiyon No	3.0
Süreç Kategorisi	
Doküman No	Viennalife_BGYS_Politikası_20240101_v3.0
Süreç Adı	BGYS
Süreç Sahibi	Bilgi Güvenliği

	İsim	Tarih
Hazırlayan	Eyüp Uyanık	01.01.2024
Onaylayan	Ömer Kara	10.01.2024
Güncelleyen	Eyüp Uyanık	31.01.2025
Onaylayan	Ömer Kara	30.06.2025
Güncelleyen	Eyüp Uyanık	29.10.2025
Onaylayan	Ömer Kara	07.11.2025

1. AMAÇ

Bu Politika, Bilgi Güvenliği Yönetim Sistemi'nin amacını, hedeflerini ve ilkelerini tanımlamak amacıyla oluşturulmuştur.

2. KAPSAM

Bu politikanın hükümleri, Viennalife personeli ile Viennalife'a özel sözleşmelerle hizmet veren veya dışarıdan destek sağlayan tedarikçi firmalar ve bunların personeli hakkında uygulanır.

3. TANIMLAR VE KISALTMALAR

Viennalife: VIENNALIFE Emeklilik ve Hayat A.Ş.

Personel: Viennalife ile iş sözleşmesine dayanarak, bütün çalışmalarını münhasıran Viennalife'a ayırmak suretiyle bağımlı olarak çalışan kişiler.

Varlık: Şirket iş süreçleri için değeri olan, kaybı ve zarar görmesi halinde işlerin aksayacağı, insan, yazılım, donanım, evrak, tesis, itibar, bilgi gibi unsurların tümü.

Bilgi Güvenliği: Bilginin yetkisiz erişimlerden korunmasını, içeriğinin yetkisiz olarak değiştirilmesinin önlenmesi ve bilginin erişim yetkisi verilen kişi ya da sistemlerce ihtiyaç duyulduğunda kullanılabilir olması.

Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini sağlamak amacıyla kurulan, işletilen ve sürekli iyileştirilen risk tabanlı yönetim sistemi.

4. GENEL İLKELER

4.1. ÇALIŞMA İLKELERİ

Bilgi Güvenliği Yönetim Sistemi, şirket hedefleri doğrultusunda;

- Şirketin tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarını korumak,
- Temel iş süreçlerinin en az hizmet kaybı ile devam etmesini sağlamak,
- Şirketin güvenilirliğini ve imajını korumak,
- Şirket çalışanlarına şirketin bilgi güvenliği gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek,
- Bilinç ve farkındalık seviyelerini artırmak ve bu şekilde şirket iş süreçlerinde ve bilgi varlıklarında oluşabilecek riskleri minimuma indirmek,
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak temel ilkeleri doğrultusunda işletilir.

Politika, çalışanlar, müşteriler, tedarikçiler ve düzenleyici otoriteler gibi ilgili tarafların bilgi güvenliği beklentileri dikkate alınarak oluşturulmuştur. BGYS amaçlarının gözden geçirilmesinden ve yeni amaçların belirlenmesinden sırasıyla BGYS Yöneticisi, Bilgi Güvenliği ve

BT Uyum Yöneticisi, BT'den sorumlu GMY ve Yönetim Komitesi sorumludur. BGYS kapsamında bilgi güvenliği hedefleri; risk değerlendirme sonuçları, yasal gereklilikler, iş hedefleri ve iç dış konular dikkate alınarak yıllık olarak belirlenir ve gözden geçirilir.

Üst Yönetim BGYS'nin etkinliğini sağlamak ve sürekli iyileştirmesini garanti altına almak amacıyla gerekli kaynakları sağlar, politika ve hedeflerin uygulanmasını destekler.

4.2. DAYANDIĞI KANUN, POLİTİKA veya YÖNETMELİKLER, İLGİLİ PROSEDÜRLER

- Erişim Kontrol Politikası
- BT İşletim Yönetimi Prosedürü
- Tedarikçi Güvenliği Politikası
- Erişim Yönetimi Politikası
- İstisna Yönetimi Prosedürü

5. HEDEFLER (KPI)

BGYS Politikası;

- Viennalife'a ait tüm bilgi varlıklarının korunmasını,
- Güvenlik uygulamalarının ihtiyaçlara cevap verecek şekilde düzenlenmesini,
- Belirlenen kural ve standartların eksiksiz bir biçimde yürütülmesini,
- Bilgi güvenliği konusunda gerek şirket çalışanlarının gerekse tedarikçi firma temsilcilerinin farkındalıklarının sağlanmasını,
- Bu bağlamda, bilgi güvenliğine yönelik eğitim ve bilgilendirmelerin düzenli olarak yapılmasını,
- Bilgi güvenliği bilginin gizliliği (need-to-know), bilgiye erişimin kesintisiz olması, bilginin bütünlüğünün bozulmaması ve temel prensipleri çerçevesinde sağlanmasını,
- Tedarikçilerle yapılan anlaşmalar ve yürütülen tüm süreçlerde belirlenen standartlara uyumun sağlanmasını,
- İç denetim birimi tarafından belirlenen takvime göre düzenli aralıklarla ve ihtiyaç duyulan durumlarda bilgi güvenliğine yönelik denetimlerin yapılmasını ya da yaptırılmasını,
- Yıllık risk değerlendirmesinin zamanında tamamlanmasını ve kritik risklerin azaltılmasına yönelik aksiyonların uygulanmasını,
- BGYS hedeflerinin yıllık olarak gözden geçirilmesini ve güncellenmesini,
- Bilgi güvenliği olaylarının %100'ü için en geç 5 iş günü içinde müdahale sürecinin başlatılmasını,

- BGYS farkındalık eğitimlerine katılım oranının yıllık %95'in üzerinde tutulmasını hedefler.

6. TEMEL RİSK ALANLARI (KRI)

Dijitalleşmeyle birlikte bilgi varlıklarına erişim kritik bir ihtiyaç haline gelmiştir. Bununla birlikte büyük oranda dijital ortamda işlenen bu bilgi varlıklarına yönelik tehditlerin sayısı, türü ve etkisi de her geçen gün artmaktadır. Bu yüzden, Viennalife'ın sahip olduğu bilgi varlıklarının, yetkisiz erişim, çalınma, bozulma, değiştirilme, kaybolma vb. her türlü tehdide karşı sistematik bir biçimde korunması gerekmektedir. Bununla birlikte her ne kadar değişen güvenlik risklerini dikkate alan dinamik bir BGYS uygulansa da zamanında belirlenemeyen ya da fark edilmesi güç olan tehditler her zaman olacaktır. Bu nedenle, altyapı ve sistem, network, yazılım, tedarikçi ve personel konularında bilgi güvenliğine yönelik risklerin tamamen ortadan kaldırılmasının mümkün olmayacağı bilinmelidir. Buna karşın BGYS, söz konusu risklerin dinamik bir biçimde güncellenerek en etkin önlemlerin alınmasını sağlar.

Bu doğrultuda, bilgi güvenliği riskleri tanımlı bir metodoloji ile düzenli olarak değerlendirilmekte ve yönetilmektedir. Her risk için ilgili risk sahipleri belirlenmekte; bu kişiler risklerin takibinden ve gerekli aksiyonların uygulanmasından sorumludur. Yasal, sözleşmesel ve dış paydaşlara ait gerekliliklerden kaynaklanan riskler de değerlendirme kapsamına dahil edilmekte; bu risklerin kabulü veya azaltılması süreçleri kayıt altına alınmaktadır. Kritik risk göstergeleri ile belirlenen alanlarda sürekli izleme yapılmakta ve bu göstergeler, yönetimin gözden geçirme toplantılarında değerlendirilerek bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi sağlanmaktadır.

7. ROL ve SORUMLULUKLAR

Bilgi Güvenliği Yöneticisi:

Şirketin tüm bilgi sistemlerinin, veri envanterinin ve dijital altyapısının her türlü siber saldırı, güvenlik açığı ve yetkisiz erişime karşı korunmasından sorumludur. Bilgi güvenliği politikalarının uygulanmasını, denetlenmesini ve sürekli iyileştirilmesini sağlar.

Ağ Güvenlik Yöneticisi: Ağ altyapısının güvenliğini sağlamak, ağ trafiğini izlemek, yetkisiz erişimleri önlemek ve gerekli güvenlik duvarı/IDS/IPS yapılandırmalarını yapmakla sorumludur.

Yönetim Komitesi: Bilgi güvenliği stratejilerinin oluşturulmasında lider rol üstlenir. Politika ve prosedürlerin onaylanması, kaynakların tahsisi, risk değerlendirmelerinin değerlendirilmesi ve sürekli iyileştirme çalışmalarının desteklenmesinden sorumludur.

Tüm Personel: Bilgi güvenliği politikalarına, prosedürlerine ve rehberlerine uymakla yükümlüdür. Güvenlik ihlali, şüpheli durumlar veya zafiyetlerle ilgili olarak derhal Bilgi Güvenliği Yöneticisini bilgilendirmekle sorumludur**.**

8. YÖNTEM ve ESASLAR

8.1. Bilgi Güvenliği İlkeleri

- Bilgi güvenliği gereksinimleri belirlenirken, Viennalife müşteri beklentileri, iç ve dış faktörler, yasa ve sözleşmelerden kaynaklanan bilgi güvenliği hususları göz önünde bulundurulur.
- Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS prosedürleri ile düzenlenir. Şirket çalışanları ve tedarikçi firmalar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.
- Bu kural ve prosedürlerin, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.
- Şirket tarafından çalışanlara veya tedarikçi firmalara sunulan bilgi sistemleri varlıkları ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça şirkete aittir.
- Çalışanların bilgi güvenliği farkındalığını artıracak ve yönetim sisteminin işleyişine katkıda bulunmalarını sağlayacak eğitimler yılda bir kez şirket çalışanlarına ve yeni işe başlayanlara verilir.
- Bilgi güvenliği olayları, ihlal ve zayıflıkları kayıt altına alınarak bu konuda şirket içi hafıza oluşturulur. Tespit edilen ihlal ve zayıflıklarla ilgili gerekli tedbirler alınıp yaptırımlar uygulanır.
- Bilgi güvenliğinde ISO 27001:2022 standardına uygun risk yönetimi yaklaşımı uygulanır. Bu amaçla, bilgi güvenliği riskleri tespit edilir, değerlendirilir ve yönetilir.
- Sistem yönetimi, ağ yönetimi, bilgi güvenliği gibi faaliyetlerde "görevler ayrılığı" prensibine uygun davranılır.
- Proje yönetimi faaliyetlerinin her aşamasında bilgi güvenliği göz önünde bulundurulur.
- Kritik bilgi teknolojileri hizmetleri ve sistemleri belirlenerek bu hizmetlerin ve sistemlerin kesintisiz hizmet verebilmesi amacıyla gerekli önlemler alınır.
- Bilgi güvenliği tehditleri ve teknolojik uygulamalar konusunda dünyadaki gelişmeler takip edilir.
- Bilgi güvenliği yönetim sistemi; performans takibi, iç denetim ve yönetimin gözden geçirmesi faaliyetleri ile sürekli iyileştirilir.
- İlk kez yapılan ya da yenilenen her tedarikçi sözleşmesinde (PoC kapsamında yapılan çalışmalar da dahil olmak üzere) ilgili çalışan ve dış taraflarla şirketin gizlilik ihtiyaçlarını güvence altına almayı amaçlayan gizlilik anlaşmaları yapılır.

- Dış taraflarla yapılacak ortak çalışmalarda güvenlik gereksinimleri analiz edilerek güvenlik şart ve kontrolleri şartname ve sözleşmelerde ifade edilir.
- Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur, risk sahiplikleri atanır.
- Şirket bilgi varlıkları sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.
- Çalışan işe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.
- Güvenli alanlar içinde saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.
- Şirkete ait bilgi varlıkları için şirket içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.
- Erişim hakları erişim politikasında tanımlandığı şekilde ve ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.

8.2. Bilgi Güvenliği Organizasyonu

- Bilgi Güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden BGYS Yönetim Temsilcisi ve Yönetim Komitesi sorumludur.
- Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesinden BGYS Yöneticisi sorumludur. BGYS Yönetim Temsilcisi ve BGYS Yöneticisi, Genel Müdür tarafından atanır.
- BGYS'nin işletilmesi ve sürdürülmesi kapsamında yapılan çalışmalar bir komite ile yürütülür. Bu maksatla, BGYS Komitesi oluşturulur.
- BGYS Komitesi, BGYS çalışmalarını gözden geçirme, eylem planı oluşturma, karar alma ve uygulama faaliyetlerini yürütmekle görevlidir.
- BGYS Komitesi, performans raporlarının değerlendirmesi veya önemli bir güvenlik ihlal olayı olması durumunda da toplanabilir.

8.3. Sorumluluklar

- Politika'nın Viennalife genelinde ve bir bütün olarak uygulanması BGYS Komitesi ve Yönetim Komitesi sorumluluğundadır.
- BGYS Yönetim Temsilcisi, Politika'nın gereklerinin yerine getirilmesi amacıyla Yönetim Komitesi'ne tavsiyelerde bulunur ve bilgi güvenliği durum raporlarının sunulmasını sağlar.
- Her bir yönetici, kendine bağlı personelin Politika'ya uygun şekilde bilgiyi korumasını temin etmekten sorumludur.

- Her bir personel, kendi işinin ve görevinin ayrılmaz bir parçası olarak bilgi güvenliği sorumluluklarını yerine getirmekle yükümlüdür.

8.4. Yönetim Desteği

- Viennalife Türkiye BGYS Komitesi ve Yönetim Komitesi, Bilgi Güvenliği Yönetim Sistemi'nin bu politikada belirtilen hedeflere uygun olarak kurulması ve işletilmesi için tüm aşamalarda destek ve kaynak sağlar.
- Bilgi güvenliği politikasını ve politikaya uygunluğun önemini çalışanlara ve ilgili dış taraflara duyurur. Bu taahhüdün sonucu olarak, şirket genelinde bilgi güvenliği farkındalık programları düzenler, danışmanlık hizmetleri alır ve gerekli yatırımları sürdürür.
- BGYS kurulurken Yönetim Komitesi tarafından BGYS Yönetim Temsilcisi ve BGYS Yöneticisi atanır.
- BGYS Yönetim Temsilcisi ve BGYS Yöneticisi değiştiğinde, işten ayrıldığında doküman revize edilerek atama tekrar yapılır.
- BGYS Yöneticisini belirlemek ve değiştirmek Yönetim Komitesi'nin yetkisindedir.
- Yönetim kademelerindeki yöneticiler güvenlik konusunda alt kademelerde bulunan çalışanlara sorumluluk verme ve örnek olma açısından yardımcı olurlar.
- Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, şirketin en alt kademe çalışanına kadar inilmesi zorunludur. Bu yüzden şirket yöneticileri gerek yazılı gerekse sözlü olarak güvenlik prosedürlerine uymaları, bilgi güvenliği ile ilgili çalışmalara katılmaları konusunda çalışanlara destek olurlar.
- Yönetim Komitesi, bilgi güvenliği kapsamındaki çalışmalar için gerek duyulan bütçeyi oluşturarak tahsis eder.

9. FORMLAR ve BELGELER

Yoktur.

10. YÜRÜRLÜLÜK ve GÜNCELLEME

İşbu BGYS Politikası yayımlandığı tarihten itibaren yürürlüğe girer ve BGYS Yöneticisi tarafından yılda bir kez kontrol edilerek gerekirse güncellenir.

11. EKLER

Yoktur.