BİLGİ GÜVENLİĞİ POLİTİKASI

FİGO TİCARİ BİLGİ VE UYGULAMA PLATFORMU A.Ş

İçindekiler

1. AMAÇ VE KAPSAM

Bu politikanın amacı, Figopara'nın (Veri Sorumlusu/Veri İşleyen) stratejik yönü ile uyumlu bilgi güvenliği prensiplerini belirleyerek tüm dijital ve fiziksel varlıklarını koruma altına almak ve temel bilgi güvenliği prensiplerini tanımlamaktır.

Bilgi güvenliği; Figopara bünyesinde yalnızca teknik bir konu olarak değil, kurumsal yönetişim, risk yönetimi, dijital operasyonel dayanıklılık, ISO 27701, ISO/27001, ISO 22301, KVKK, PCI DSS standartları ve sürdürülebilirlik yaklaşımının ayrılmaz bir parçası olarak ele alınır. Bu politika, bilgi güvenliği uygulamalarının Avrupa Birliği dijital dayanıklılık düzenlemeleri, OECD, DORA, ESG yönetişim ilkeleri, ISO standartları ve uluslararası iyi uygulamalarla uyumlu şekilde yürütülmesini esas alır.

Entegre Yönetim Sistemimizin (EYS) bir parçası olarak, Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) kurulması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi yönetimin yönlendirmesi doğrultusunda yürütülür. Figopara'nın bilgi güvenliğine ilişkin yaklaşımı ve hedefleri; bilgi güvenliği yönetim sistemi gereklilikleri çerçevesinde tanımlanır ve bu gereklilikler ile hedeflerin tüm çalışanlara ve ilgili paydaşlara etkin şekilde duyurulması amaçlanır.

Bu politika,tüm bilgi varlıklarını (elektronik veya basılı formlardaki BGYS ile ilgili tüm politikalara, prosedürlere, formlara, kayıtlara vb. dokümanlar) ve çalışanlarını ve bilgi güvenliğiyle ilgili tüm belgeler ile bilgi ve iletişim teknolojileri (ICT) varlıklarını, bu varlıklar üzerinden sunulan kritik hizmetleri, üçüncü taraflar aracılığıyla sağlanan bilgi teknolojisi hizmetlerini ve bunların kurumun operasyonel dayanıklılığı üzerindeki etkilerini de kapsar.

Tüm Paydaşlar (çalışanlar, yöneticiler, iş ortakları vb.) ve ilgili taraflar bu politikaya uymakla yükümlüdür.

2. TANIMLAR VE KISALTMALAR

BGYS: Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Standartları: Bilgi güvenliği standartları, şirketlerinn bilgi varlıklarını koruma, güvenliğini sağlama ve bilgiye yetkisiz erişimi önleme amacıyla belirlenmiş kurallar, yönergeler ve uygulama kriterleridir. Bu standartlar, bilgi güvenliği yönetim sistemlerinin (BGYS) kapsamını ve gereksinimlerini tanımlar ve bu sistemlerin güvenilirlik, gizlilik, bütünlük ve erişilebilirlik ilkelerine uygun olarak nasıl kurulması ve işletilmesi gerektiğini belirler.

EYS Ekibi (Entegre Yönetim Sistemi Ekibi): EYS ekibi yönetimi temsil eden, Entegre Yönetim sistemi kapsamında yer alan BGYS'nin başarılı biçimde sürdürülebilmesi için sorumluluğu üstlenen ve gözetimini sağlayan ekiptir.

Veri Sorumlusu: Kişisel verilerin işlenme amaçlarını ve bu veriler üzerinde yapılacak işlemleri belirleyen ve karar veren gerçek veya tüzel kişidir.

Veri İşleyen: Veri sorumlusunun talimatları doğrultusunda kişisel verileri işleyen gerçek veya tüzel kişidir.

İç Denetçi: EYS'nin bağımsız olarak denetimini yapan kişi veya ekip. EYS'nin uygulanmasından ve işletiminden bağımsız, EYSkapsamındaki Yönetim Sistemlerinin denetimini yerine getirebilecek deneyim, eğitim ve sertifikasyonlara sahip kişi olup; iç denetimi gerçekleştiren kişidir. İç denetçi şirket personeli olabileceği gibi şirket dışından da sağlanabilir.

Paydaş: Figopara'nın bilgi güvenliği kapsamındaki faaliyetleriyle ilişkili olan veya bu faaliyetlerden etkilenen çalışanlar, yöneticiler, iş ortakları, tedarikçiler, hizmet sağlayıcılar ve üçüncü taraflardır.

Müşteri: Figopara'nın sunduğu ürün ve hizmetlerden yararlanan, Figopara ile sözleşmesel ilişki içinde bulunan veya hizmetlerin sunulması kapsamında kendisine ait veriler işlenen gerçek veya tüzel kişiyi ifade eder.

ISO: (International Organization for Standardization) ürünlerin ve hizmetlerin kalite, güvenlik, verimlilik ve uyumluluk açısından belirli kriterlere göre yürütülmesini sağlayan uluslararası standartlar bütünüdür.

DORA (Digital Operational Resilience Act): Avrupa Birliği finansal kuruluşlarının bilgi ve iletişim teknolojileri kaynaklı operasyonel risklere karşı dayanıklılığını güçlendirmeyi amaçlayan düzenlemedir.

ESG (Environmental, Social, Governance): Kurumsal sürdürülebilirlik kapsamında çevresel, sosyal ve yönetişim faktörlerini içeren çerçevedir.

Dijital Operasyonel Dayanıklılık: Bilgi sistemleri, süreçler ve üçüncü taraf bağımlılıkları dâhil olmak üzere, dijital operasyonların kesintilere karşı sürdürülebilir şekilde devam edebilme yeteneğidir.

ICT (Information and Communication Technologies): Bilgi ve İletişim Teknolojileri- Figopara'nın faaliyetlerini yürütmek, hizmet sunmak, veri işlemek, depolamak, iletmek veya erişilebilir kılmak amacıyla kullandığı bilgi sistemleri, yazılımlar, donanımlar, ağ altyapıları, dijital platformlar, uygulamalar, veri merkezleri, bulut hizmetleri ve bunlarla ilişkili teknolojik bileşenlerin tümünü ifade eder.

3. ROLLER VE SORUMLULUKLAR

3.1. Üst Yönetim

Üst Yönetim, bilgi güvenliği, dijital operasyonel dayanıklılık, kişisel verilerin korunması ve iş sürekliliğini kurumsal yönetişim, risk yönetimi ve sürdürülebilirlik yaklaşımının ayrılmaz bir parçası olarak ele alır; bu alanların DORA, ESG ilkeleri, ISO/IEC 27001, ISO/IEC 27701, ISO 22301, KVKK ve PCI DSS ile uyumlu şekilde yönetilmesinden nihai olarak sorumludur. Üst Yönetim, Bilgi Güvenliği Politikasının kurum ihtiyaçlarını karşılar nitelikte olmasını, uygulanması için gerekli kaynak ve desteğin sağlanmasını ve politikanın en az yılda bir kez veya gerekli görülen durumlarda gözden geçirilerek onaylanmasını sağlar.Üst yönetimi temsilen bu görevi Yönetim Temsilcisi yapar ve Genel Müdür'e onaylatır.

3.2. Yönetim Temsilcisi

Üst Yönetimi temsilen Bilgi Güvenliği Yönetim Sistemi'nin kurulması, uygulanması, izlenmesi, yönetilmesi ve sürekli iyileştirilmesini koordine eden kişidir. Bilgi güvenliği ve dijital operasyonel dayanıklılık risklerini izler, BGYS performansını Üst Yönetime raporlar ve politika ile ilgili gerekli güncellemeleri Yönetim Kurulu ve/veya Genel Müdür onayına sunar.

3.3. EYS Ekibi

Şirket'in üst yönetimi tarafından görevlendirilen EYS ekibi, Bilgi Güvenliği Politikasının Şirket ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya kurum politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur.
EYS Ekibi, bilgi güvenliği uygulamalarının uluslararası standartlara, kurumsal sürdürülebilirlik, yönetişim ve operasyonel dayanıklılık hedefleriyle uyumlu şekilde yürütülmesini gözetir.

3.4. Tüm Personel

Bilgi Güvenliği Politikasının gereklerinin görev alanlarının gerektirdiği biçimde yerine getirilmesinden sorumludur.

4. ÜST YÖNETİM TAAHHÜDÜ

Figopara Üst Yönetimi, EYS/BGYS sürecinde kurumun hedef ve politikalarını gerçekleştirmek için DORA, ESG sürdürülebilirlik, IFC Guideline, OECD, NIS2, GDPR, ISO/IEC 27001, 27701, 22301 ve benzeri bilgi güvenliği standartları ile yasal yükümlülüklerde yer alan tüm gereksinimlerin yerine getirilecek şekilde kurulmasını ve işletilmesini taahhüt eder.

Figopara Üst Yönetimi, yayımlanmış ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları ve gerekli altyapı yatırımlarını tahsis edeceğini, sürecin etkinliğini sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder.

Figopara Üst Yönetimi, bilgi güvenliğini dijital operasyonel dayanıklılığın temel unsurlarından biri olarak kabul eder; bilgi güvenliği ihlallerini yalnızca teknik bir konu olarak değil, aynı zamanda uluslararası standartlara uyum, kurumsal yönetişim, itibar ve sürdürülebilirlik açısından risk teşkil eden hususlar olarak ele almayı taahhüt eder.

Üst yönetim, bilgi ve iletişim teknolojileri (ICT) kaynaklı risklerin yönetilmesi ile dijital operasyonel dayanıklılığın sağlanmasına ilişkin çerçevenin oluşturulması, uygulanması ve gözetiminden nihai olarak sorumludur.

Figopara, bilgi güvenliği ve siber tehditlere ilişkin bilgilerin, yürürlükteki mevzuat ve gizlilik yükümlülükleri çerçevesinde, ilgili taraflarla kontrollü ve sorumlu şekilde paylaşılmasını sağlar.

5. POLİTİKA

Figopara, verilerinin ve sistemlerinin yeterince korunması ve bilgi teknolojilerinin işleyişiyle ilişkili her türlü güvenlik riskinin yönetilmesi için yasal ve ticari sorumluluklara sahiptir. Figopara, bilgi ve iletişim sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini garanti altına almak, güvenlik risklerini yönetmek, operasyonel ve finansal verilerini korumak için yasal gereklilikler, DORA, ESG sürdürülebilirlik, IFC Guideline, OECD, NIS2, GDPR, ISO/IEC 27001, 27701, 22301 ve benzeri bilgi güvenliği standartlara uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamayı hedefler. Bilgi güvenliği uygulamaları, risk bazlı ve orantılı bir yaklaşımla yürütülür. Alınan önlemler, bilginin niteliği, hassasiyeti ve kurum faaliyetleri üzerindeki etkisi dikkate alınarak belirlenir.

ISO 27001, 27701 ve benzeri bilgi güvenliği standartları Bilgi Güvenliği Yönetim Sistemi gerekliliklerine uygun olarak, risk bazlı düşünme yaklaşımı ile gerçekleştirdiğimiz ve sürekli iyileştirdiğimiz süreçlerimiz sayesinde, sunduğumuz ürün ve hizmetlerin müşterilerimizin ihtiyaç ve beklentilerini karşılanmasını, çalışanlarımız, müşterilerimizin, tedarikçilerimizin ve iş ortaklarımızın bilgilerinin gerekli şekilde korunmasını taahhüt edip güvence altına almaktayız.
Figopara tarafından onaylanmış olan bu Bilgi Güvenliği Politikasının amacı;

- İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı kuruluşun bilgi varlıklarını korumak,

- Bilginin gizliliğini ve bütünlüğünü bozmaya çalışacak yetkisiz kişilerin erişimine karşı korumak,
- Bilgiye erişilebilirliği iş süreçleriyle gerektiği şekilde sağlamak,
- DORA, ESG, OECD, IFC, NIS2, GDPR ve ISO/IEC 27701 ile 27001 standartlarına uyumu sağlamak,
- Yasal mevzuat gereksinimlerini karşılamak,
- İş sürekliliği ve Kriz Yönetimi için planları hazırlamak, sürdürmek ve test etmek,
- Tüm çalışanların bilgi güvenliği eğitimlerine katılımını ve BGYS farkındalığını sağlamak,
- Bilgi Güvenliği Yönetim Sisteminin etkin bir şekilde yönetilmesini sağlamak amacıyla risk analizi çalışmalarını yapmak,
- Bilgi güvenliği risklerini yönetmek için riskleri değerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirmek, gerekli tedbirleri geliştirmek ve olası riskleri önlemek için çalışmalar yapmak,
- Bilgi güvenliğindeki gerçekte var olan veya şüphe uyandıran tüm açıkları, Etik & İhlal Yönetim platformu aracılığıyla bildirmek ve Etik & İhlal Komitesi tarafından soruşturulmasını sağlamak,
- Bilgiye erişilebilirlik ve bilgi sistemleri için iş gereksinimlerini karşılamak,
- Kapsamda yer alan süreçleri Bilgi Güvenliği Yönetim Sistemi'ne uygun hale getirmek,
- Bilgi güvenliği yönetim sistemimizin amaçlanan sonuçları yerine getirme başarısını periyodik olarak gözden geçirmek, gerekli iyileştirmelerin zamanında hayata geçirilmesini güvence altına almak
- Bilgi güvenliğini dijital operasyonel dayanıklılığın temel unsurlarından biri olarak ele almak ve bilgi ve iletişim teknolojileri (ICT) kaynaklı risklerin kurumsal faaliyetler üzerindeki etkilerini yönetmek,
- Bilgi güvenliği ve ICT kaynaklı risklerin yönetimine ilişkin üst yönetim gözetimini ve hesap verebilirliği sağlamak,
- Üçüncü taraflar ve hizmet sağlayıcılar aracılığıyla yürütülen faaliyetlerde bilgi güvenliği ve dijital operasyonel dayanıklılık risklerini yönetmek,
- Bilgi güvenliği olaylarının ve siber güvenlik vakalarının, ilgili mevzuat kapsamında doğabilecek bildirim ve raporlama yükümlülükleri çerçevesinde ele alınmasını sağlamaktır.

Şirket bünyesindeki BGYS kapsamında yayımlanan tüm dokümanlar, Bilgi Güvenliği Politikasını destekler. Yönetim Temsilcisi bu politikanın sürdürülmesinden ve politikanın gerçekleştirilmesi konusunda tavsiyelerde bulunmaktan, yol göstermekten doğrudan sorumludur ve yetkili otoritedir.

6. GENEL İLKE VE ESASLAR

6.1. Dijital Operasyonel Dayanıklılık İlkesi

Figopara, bilgi güvenliğini dijital operasyonel dayanıklılığın ayrılmaz bir unsuru olarak ele alır. Bilgi ve iletişim teknolojileri (ICT) kaynaklı riskler, Figopara'nın kurumsal risk yönetimi ve operasyonel dayanıklılık çerçevesine entegre edilir ve üst yönetimin aktif gözetimi altında yönetilir.

Kritik bilgi sistemlerinin ve bu sistemler üzerinden sunulan hizmetlerin sürekliliğinin korunması, Figopara açısından temel bir kurumsal önceliktir.

Bilgi güvenliği olayları ve siber güvenlik vakaları, kurumun operasyonel dayanıklılığını etkileyebilecek riskler olarak değerlendirilir ve ilgili mevzuat kapsamında yetkili otoritelere bildirim yükümlülüğü doğurabilecek nitelikteki olaylar dikkate alınır.

6.2. ICT Risk Yönetimi ve Olaylara Hazırlık

Bilgi güvenliği riskleri, Figopara'nın kurumsal risk envanterinin ayrılmaz bir parçası olarak ele alınır.

Bu risklerin belirlenmesi, değerlendirilmesi ve yönetilmesi risk bazlı ve orantılı bir yaklaşımla yürütülür.

Bilgi güvenliği olaylarının yönetimi, kurumsal risk yönetimi ve şeffaflık ilkeleri doğrultusunda ele alınır. Olayların sınıflandırılması, bildirimi ve müdahalesine ilişkin detaylar ilgili prosedürler aracılığıyla düzenlenir.

6.3. Üçüncü Taraf ve ICT Hizmet Sağlayıcı Yönetimi

Üçüncü taraflar ve hizmet sağlayıcılar aracılığıyla erişilen bilgi ve sistemler, Figopara'nın bilgi güvenliği ilkelerine tabidir.

Dijital operasyonel dayanıklılık açısından kritik nitelikte olan üçüncü taraf hizmet sağlayıcılar, bilgi güvenliği ve operasyonel risk perspektifiyle ayrıca değerlendirilir.

Üçüncü taraflarla kurulan sözleşmelerde bilgi güvenliği, denetim ve gerekli hâllerde fesih hakları gözetilir.

6.4. İş Sürekliliği ve Bilgi Güvenliği Entegrasyonu

Bilgi güvenliği, Figopara'nın iş sürekliliği yaklaşımının temel bileşenlerinden biridir.

Kritik bilgi varlıklarının ve bilgi sistemlerinin sürekliliğinin korunması, iş sürekliliği hedefleriyle bütünleşik şekilde ele alınır.

İş sürekliliği, felaket kurtarma, test ve tatbikatlara ilişkin detaylar ilgili prosedürler kapsamında düzenlenir.

6.5. Kurumsal Yönetişim, Hesap Verebilirlik ve ESG Yaklaşımı

Bilgi güvenliği, Figopara'nın kurumsal yönetişim ve ESG (Environmental, Social, Governance) yaklaşımının ayrılmaz bir parçasıdır.

Üst yönetim, bilgi güvenliği risklerinin yönetilmesi konusunda hesap verebilirliğe sahiptir.

Bilgi güvenliği uygulamaları, kurumsal şeffaflık, hesap verebilirlik ve etik yönetim ilkeleriyle uyumlu şekilde yürütülür.

Bilgi güvenliği ihlalleri yalnızca teknik bir konu olarak değil; aynı zamanda yönetişim, itibar ve sürdürülebilirlik riski olarak değerlendirilir.

6.6. Veri Etiği, Gizlilik ve Müşteri Bilgilerinin Korunması

Veri güvenliği ve gizliliği, Figopara'nın paydaş güveninin korunmasına yönelik temel sorumluluklarındandır.

Kişisel veriler, finansal müşteri bilgileri ve ticari sırlar yüksek hassasiyetli bilgi varlıkları olarak kabul edilir ve amaçla sınırlılık, yetkilendirme ve gizlilik ilkeleri çerçevesinde ele alınır.

Yetkisiz erişimlerin önlenmesi ve veri güvenliğinin sağlanması, kurumsal etik yükümlülüğün bir parçasıdır.

6.7. Sürekli İzleme ve Yönetimin Bilgilendirilmesi

Bilgi güvenliği ile ilgili riskler, önemli gelişmeler ve ortaya çıkan tehditler, üst yönetimin bilgilendirilmesini sağlayacak şekilde ele alınır.

Bilgi güvenliği yönetimi, değişen tehdit ortamı ve kurumsal ihtiyaçlar doğrultusunda sürekli gözden geçirilir ve geliştirilir.

6.8. Standartlara Uyumun Sağlanması

ISO/IEC 27001 standardı kapsamında tanımlanan kontrol hedefleri ve kontroller, Figopara bünyesinde ilgili prosedürler aracılığıyla uygulanır.

7. İLGİLİ DOKÜMANLAR

7.1. Dahili Dokümanlar

1. Kapsam Analizi Dokümanı
2. Entegre Yönetim Sistemi Politikası
3. Bilişim Teknolojileri Yönetim Politikaları

4. Kabul Edilebilir Kullanım Politikası

7.2. HARİCİ DOKÜMANLAR

1. Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA)
2. Directive (EU) 2022/2555 – NIS2
3. OECD Recommendation on Digital Security Risk Management
4. IFC Information Security & Risk Governance Guidelines
5. ISO / IEC 27001: 2022 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler
6. ISO 27701:2019 KVYS Kişisel Veri Yönetim Sistemi – Gereksinimler
7. ISO 22301:2019 İş Sürekliliği Yönetimi Sistemi – Gereksinimler
8. Kişisel Verileri Koruma Kurumu Veri Güvenliği Rehberi (İdari ve Teknik Tedbirler)

8. DAĞITIM

Bu dokuman elektronik ortamda tüm paydaşlarla paylaşılmaktadır.

9. YAPTIRIM

Bu dokumana aykırı davranılması durumunda **Disiplin Prosedürü** dikkate alınarak işlem yapılacaktır.

9.1. UYUM

Bu politikanın ihlali, veri koruma mevzuatı kapsamındaki veri ihlallerine, şirketin itibarının zarar görmesine ve çalışanların veya diğer ilgili üçüncü şahısların haklarının ihlal edilmesine neden olabilir.

9.2. İSTİSNALAR

Politika ile ilgili herhangi bir istisna, önceden Genel Müdür ve / veya Veri Sorumlusunun kendisine bildirilecektir.

9.3. UYUMSUZLUK

Bu politikalara uyulmaması, Şirketin disiplin prosedürlerine uygun olarak disiplin cezasına yol açabilir. Üçüncü taraf bir yüklenicinin (veya alt yüklenicilerin) bu politikaya uymaması, sözleşmenin ve / veya yasal işlemin feshine yol açabilir. Uygunsuzluk, Genel Müdür ve / veya Veri Sorumlusunun kendisine bildirilecektir.