1 AMAÇ VE KAPSAM

Bu politikanın amacı, Figopara'nın stratejik yönü ile uyumlu bilgi güvenliği prensiplerini belirleyerek tüm dijital varlıklarını koruma altına almak ve temel bilgi güvenliği prensiplerinin tanımlanmasıdır. BGYS'nin kurulması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi için yönetimin yönlendirmesi, iç ve dış paydaşların her türlü bilgi güvenliği yönetim sistemi gereksinimlerine ilişkin Figopara'nin bilgi güvenliği yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili paydaşlara bu gereklilik ve hedefleri açıkça bildirmektir.

Bu politikanın gereklilikleri, tüm bilgi varlıklarını (elektronik veya basılı formlardaki BGYS ile ilgili tüm politikalara, prosedürlere, formlara, kayıtlara vb. dokümanlar) ve çalışanlarını ve bilgi güvenliğiyle ilgili tüm belgelerini kapsar.

Tüm çalışanlar, yöneticiler, iş ortakları 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.

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.

3 ROLLER VE SORUMLULUKLAR

Üst Yönetim

Bilgi Güvenliği Politikasının kurum ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya şirket politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur. Üst yönetimi temsilen bu görevi Yönetim Temsilcisi yapar ve Genel Müdür'e onaylatır.

Yönetim Temsilcisi

Bilgi Güvenliği Yönetim sisteminin kurulmasından işletilmesi ve yönetilmesine dek her aşamada üst yönetime karşı sorumluluk üstlenen kişidir.

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.

Tüm Personel

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

4 ÜST YÖNETİM TAAHHÜDÜ

Figopara Üst Yönetimi, BGYS sürecinde kurumun hedef ve politikalarını gerçekleştirmek için ISO/IEC 27001, 27701 ve benzeri bilgi güvenliği standartlar 'da 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.

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 için ISO/IEC 27001, 27701 ve benzeri bilgi güvenliği standartlara uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamayı hedefler.

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,
- 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, Bilgi Güvenliği Yöneticisine rapor etmek ve Bilgi Güvenliği Yöneticisi 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 almaktır.

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 İLGİLİ DOKÜMANLAR

6.1 Dahili Dokümanlar

1. Kapsam Analizi Dokümanı

6.2 Harici Dokümanlar

1. ISO / IEC 27001: 2022 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler
2. ISO 27701:2019 KVYS Kişisel Veri Yönetim Sistemi - Gereksinimler

3. ISO 22301:2019 İş Sürekliliği Yönetimi Sistemi - Gereksinimler
4. Kişisel Verileri Koruma Kurumu Veri Güvenliği Rehberi (İdari ve Teknik Tedbirler)

7 DAĞITIM

Bu dokuman elektronik ortamda tüm çalışanlarla paylaşılmaktadır.

8 YAPTIRIM

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

8.1 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.

8.2 İSTİSNALAR

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

8.3 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.