

**İÇİNDEKİLER**

1. AMAÇ .....	2
2. KAPSAM.....	2
3. TANIMLAR .....	2
4. SORUMLULUK.....	3
5. BİLGİ GÜVENLİĞİ HEDEFLERİ.....	6
6. RİSK YÖNETİM ÇERÇEVESİ.....	6
7. BİLGİ GÜVENLİĞİ GENEL ESASLARI .....	6
8. POLİTİKANIN İHLALİ VE YAPTIRIMLAR.....	8
9. YÖNETİMİN GÖZDEN GEÇİRMESİ.....	9
10. BİLGİ GÜVENLİĞİ POLİTİKA DOKÜMANI GÜNCELLENMESİ VE GÖZDEN GEÇİRİLMESİ	9

**KONTROLÜ KOPYADIR**

<b>HAZIRLAYAN</b> BGYS Temsilcisi	<b>KONTROL EDEN</b> Kurumsal Yönetim	<b>ONAYLAYAN</b> Yönetim Kurulu Başkanı

## 1. AMAÇ

Bu politikanın amacı, YÖRPAŞ YÖRESEL YİYECEKLER PAZARLAMA A.Ş.'nin ("YÖRPAŞ/Şirket") kendisinin ve hizmet verdiği müşterilerine sağladığı ve YÖRPAŞ'ın fiziksel çerçevesi içerisinde, ISO 27001 standart kapsamında hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklerine ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için Üst Yönetimin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

## 2. KAPSAM

YÖRPAŞ'ın bünyesinde yapılan ticari faaliyetlere ve bu işlemlere ilişkin bilgi sistemleri, muhasebe, raporlama, operasyon, müşteri ilişkileri, şikayet, risk yönetimi, iç yönetim faaliyetlerinden elde edilen elektronik bilgi varlıklarının korunması, şirket bünyesinde tutulan kişisel verilerin kanun kapsamında işlenmesi, saklanması, korunması, gizliliğinin ve bütünlüğünün bozulmaması için kullandığı bilgi güvenliği süreçlerini kapsar.

## 3. TANIMLAR

**BGYS** : Bilgi Güvenliği Yönetim Sistemi

**BGYS El Kitabı**: Bilgi Güvenliği hakkında çalışanları bilgilendirmek, amaçları belirlemek için hazırlanan bilgilendirme kitapçığı

**Envanter** : Yörpaş için önemli olan her türlü bilgi varlığı

**Know-How** : Bir şeyi yapabilme yetkinliği

**Bilgi Güvenliği** : Bilgi, tüm diğer kurumsal ve ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun şekilde korunması gereken bir varlıktır. Yörpaş içerisinde, know-how, süreç, formül,

HAZIRLAYAN BGYS Temsilcisi	KONTROL EDEN Kurumsal Yönetim	ONAYLAYAN Yönetim Kurulu Başkanı

teknik ve yöntem, müşteri kayıtları, pazarlama ve satış bilgileri, personel bilgileri, ticari, sınai ve teknolojik bilgiler ve sırlar GİZLİ BİLGİ olarak kabul edilir.

**Gizlilik** : Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Örnek: Şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir Kayıtlı elektronik posta – KEP)

**Bütünlük** : Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Örnek: Veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması - elektronik imza - mobil imza)

**Erişilebilirlik/Kullanılabilirlik:** Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Diğer bir ifadeyle, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır.

**Bilgi Varlığı** : Yörpaş'ın sahip olduğu, faaliyetlerini aksatmadan yürütebilmesi için önemli olan varlıklardır. Bu politikaya konu olan süreçler kapsamında bilgi varlıkları şunlardır:

- Kağıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri,
- Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım,
- Bilginin transfer edilmesini sağlayan ağlar,
- Tesisler ve özel alanlar,
- Bölümler, birimler, ekipler ve çalışanlar,
- Çözüm ortakları,
- Üçüncü taraflardan sağlanan servis, hizmet veya ürünlerdir.

#### 4. SORUMLULUK

Sorumluluk ve yetkileri belirlenmiş görevlerin nitelik ve yeterlilikleri görev tanımlarında tanımlanmıştır. Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Bilgi Sistemleri Yönetim Temsilcisi Sorumludur.

BGYS Yönetim Temsilcisi Yönetim Kurulu Başkanı tarafından atanır.

HAZIRLAYAN BGYS Temsilcisi	KONTROL EDEN Kurumsal Yönetim	ONAYLAYAN Yönetim Kurulu Başkanı

#### 4.1. Yönetim Sorumluluğu

4.1.1. Yörpaş Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli kaynakları tahsis edeceğini, sistemin tüm çalışanlar tarafından anlaşılmasının sağlayacağını taahhüt eder.

4.1.2. BGYS kurulumu sırasında Yönetim Temsilcisi atama yazısı ile atanır. Gerekli olduğu durumlarda Yönetim Kurulu tarafından doküman revize edilerek atama tekrar yapılır.

4.1.3. Yönetim kademesindeki yöneticiler güvenlik konusunda alt kademelerde bulunan çalışana sorumluluk verme ve örnek olma açısından yardımcı olurlar. Yönetim Kurulundan başlayan ve uygulanan anlayış, Yörpaş'ın en alt kademe çalışanına kadar inilmesi zorunludur. Bu yüzden tüm yöneticiler yazılı ya da sözlü olarak güvenlik talimatlarına uymaları, güvenlik konularındaki çalışmalara katılmaları yönünde çalışanlarına destek olurlar.

4.1.4. Yönetim Kurulu, Bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

#### 4.2. BGYS Yönetim Temsilcisi Sorumluluğu ve Görevleri

4.2.1. BGYS Politikası ve Hedefleri doğrultusunda çalışmak,

4.2.2. Bilgi Güvenliği Yönetim Sistemi için gerekli dokümanların oluşturulmasını, uygulanmasını ve sürekliliğinin sağlanmasını organize etmek,

4.2.3. Bilgi Güvenliği Yönetim Sistemi'nin performansı ve iyileştirilmesi için herhangi bir ihtiyaç olduğunda Üst Yönetime rapor vermek,

4.2.4. Prosedürlerin hazırlanmasını temin etmek, BGYS Sistemine uygunluğu açısından inceleyip onaylamak,

4.2.5. Yörpaş çalışanlarını BGYS konusunda bilinçlendirmek için her seviyede çeşitli eğitimler vermek,

4.2.6. Kuruluşta, müşteri şartlarının bilincinde olunmasının yaygınlaştırılmasını sağlamak,

HAZIRLAYAN BGYS Temsilcisi	KONTROL EDEN Kurumsal Yönetim	ONAYLAYAN Yönetim Kurulu Başkanı

- 4.2.7. Bilgi Güvenliği Yönetim Sistemi ile ilgili konularda kuruluş dışında da iş birliği yapmak,
- 4.2.8. Tüm birimlerin bilgi işlem kalite hedef ve politikasına uygun çalışmalarını sağlamak ve koordinasyonu kurmak,
- 4.2.9. Prosedürleri, talimatları ve formları hazırlamak ya da kontrol ederek Yönetim Kurulu Başkanı onayına sunmak,
- 4.2.10. Düzeltici faaliyetlerin uygun kanallardan başlatılmasını, yürütülmesini ve izlenmesini sağlamak,
- 4.2.11. Bilgi Güvenliği Yönetim Sistemi kapsamındaki tüm fonksiyonların yılda en az 1 defa olmak üzere tetkikten geçirilmesi için iç tetkik çalışmalarını planlamak ve takip etmek,
- 4.2.12. İç tetkik bulgularını Yönetimin Gözden Geçirilmesi Toplantısı gündemine taşımak,
- 4.2.13. Yönetimin Gözden Geçirilmesi Toplantısında alınan kararların uygulamalarını takip etmek.
- 4.2.14. Bilgi Güvenliği Yönetim Sistemi Kayıtlarının yönetimi ve kontrol altında tutulması işlerini yürütmek.
- 4.2.15. Bilgi İşlemin genel çalışma kurallarına uygun hareket etmek.

**4.3. Bilgi Teknolojileri Sorumlusu Görevleri**

- 4.3.1. Bilgi işlem yönetimini gerçekleştirmek,
- 4.3.2. Bütçe planlamasını yapmak,
- 4.3.3. BGYS Politikası ve Hedefleri doğrultusunda çalışmak,
- 4.3.4. Yönetimin Gözden Geçirilmesi Toplantısında alınan kararların uygulamalarını takip etmek,
- 4.3.5. Bilgi Güvenliği Yönetim Sistemi Kayıtlarının yönetimi ve kontrol altında tutulması işlerini yürütmek,
- 4.3.6. Bilgi İşlemin genel çalışma kurallarına uygun hareket etmek,
- 4.3.7. Politika, Prosedür ve talimatlarda kendisine verilen görevleri yerine getirmek.

HAZIRLAYAN BGYS Temsilcisi	KONTROL EDEN Kurumsal Yönetim	ONAYLAYAN Yönetim Kurulu Başkanı

## 5. BİLGİ GÜVENLİĞİ HEDEFLERİ

Kritik öneme sahip sistemlerinde yer alan tüm bilgi varlıklarını korumayı, bilgi güvenliği çerçevesinde mevzuatla, sözleşmelerle ve uluslararası standartlarla uyumlu çalışmayı, Bilgi Güvenliği Yönetim Sistemindeki riskleri yönetmeyi, düzeltici ve iyileştirici faaliyetlerde bulunmayı ve kuruluş amacına uygun olarak sürdürülebilir bir sistem kurmayı hedefler. Üst Yönetim tarafından belirlenen hedefler belirlenmiş periyotlarda izlenir ve Yönetim Gözden Geçirme toplantılarında gözden geçirilir.

## 6. RİSK YÖNETİM ÇERÇEVESİ

Yörpaş risk yönetim çerçevesi; Bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Risk Analizi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar. Risk işleme planının yönetiminden ve gerçekleştirilmesinden BGYS Yönetim Temsilcisi sorumludur. Tüm bu çalışmalar, varlık envanteri ve risk değerlendirme prosedüründe detaylı olarak açıklanır.

## 7. BİLGİ GÜVENLİĞİ GENEL ESASLARI

- 7.1. Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar belirlenmiştir. Yörpaş çalışanları ve üçüncü taraflar bu politika ve prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.
- 7.2. Bu kural ve politikaların, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.
- 7.3. Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001 "Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimler

HAZIRLAYAN BGYS Temsilcisi	KONTROL EDEN Kurumsal Yönetim	ONAYLAYAN Yönetim Kurulu Başkanı

(Information Security Management Systems Requirements)" standardını temel alarak yapılandırılır ve işletilir.

- 7.4. BGYS'nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların katkısıyla yürütür. BGYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yönetim Temsilcisi sorumluluğundadır.
- 7.5. Yörpaş tarafından çalışanlara veya üçüncü taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça Yörpaş'a aittir.
- 7.6. Çalışanlar, danışmanlık, hizmet alımı yapılan (Güvenlik, servis, yemek, temizlik firması vb.), Tedarikçiler ve Stajyerler ile gizlilik anlaşmaları yapılır.
- 7.7. İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.
- 7.8. Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut Yörpaş çalışanlarına ve yeni işe başlayan çalışanlara verilir.
- 7.9. Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.
- 7.10. Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.
- 7.11. Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.
- 7.12. Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.

HAZIRLAYAN BGYS Temsilcisi	KONTROL EDEN Kurumsal Yönetim	ONAYLAYAN Yönetim Kurulu Başkanı

- 7.13. Yörpaş'a ait bilgi varlıkları için firma içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.
- 7.14. Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.
- 7.15. Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır.
- 7.16. Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.
- 7.17. Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
- 7.18. Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.  
Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.

## 8. POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Bilgi Güvenliği Politikasına ve Standartlarına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar için Yörpaş Disiplin Prosedüründe belirlenen yaptırımlar uygulanır.

HAZIRLAYAN BGYS Temsilcisi	KONTROL EDEN Kurumsal Yönetim	ONAYLAYAN Yönetim Kurulu Başkanı

## 9. YÖNETİMİN GÖZDEN GEÇİRİLMESİ

Yönetim gözden geçirme toplantıları BGYS Yönetim Temsilcisi tarafından organize edilerek, Yönetim Kurulu ve Birim Sorumluları katılımı sağlanır. Bilgi Güvenliği Yönetim Sisteminin uygunluğunun ve etkinliğinin değerlendirildiği bu toplantılar en az yılda bir kez gerçekleştirilmektedir.

## 10. BİLGİ GÜVENLİĞİ POLİTİKA DOKÜMANI GÜNCELLENMESİ VE GÖZDEN GEÇİRİLMESİ

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yönetim Temsilcisi sorumludur. Politika ve prosedürler en az yılda bir kez gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa Üst Yönetime onaylatılarak yeni versiyon olarak kayıt altına alınmalıdır. Her revizyon tüm kullanıcıların erişebileceği şekilde yayınlanmalıdır.

**KONTROLLÜ KOPYADIR.**

<b>HAZIRLAYAN</b> BGYS Temsilcisi	<b>KONTROL EDEN</b> Kurumsal Yönetim	<b>ONAYLAYAN</b> Yönetim Kurulu Başkanı