SMARTYARN TEKNOLOJİLERİ TEKSTİL SAN. ve TİC. A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

SMARTYARN BİLGİ GÜVENLİĞİ POLİTİKASI

Belge Adı : SMARTYARN Bilgi Güvenliği Politikası

Kapsamı : Smartyarn tarafından kişisel verileri işlenen çalışanlar ve tüm gerçek kişiler,

Hazırlayan : Hukuk Müşavirliği / Bilgi İşlem

Tarih/ Versiyon : **16/11/2020**

Onaylayan : Smartyarn KVK Kurul yöneticileri tarafından onaylanmıştır.

Revizyon Nedeni:	Hazırlayan	Kontrol Eden	Onaylayan
	Bilgi İşlem Ekibi	Bilgi İşlem Sorumlusu / Hukuk Birimi	Genel Müdür

BİLGİ GÜVENLİĞİ POLİTİKASI

1. **Amaç :** Bu politikanın amacı, hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek ve 6698 sayılı Kişisel Verileri Koruma Kanunu uyarınca kişisel verilerin güvenliğini sağlamak için, üst yönetimin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

2. **Kapsam :** Bu politika Şirket bünyesinde yapılan ticari faaliyetlere ve bu işlemlere ilişkin lojistik, depolama, muhasebe, finans, kalite güvence, satın alma, insan kaynakları, hukuk, satış, pazarlama, iç denetim ve bilgi işlem faaliyetlerinden elde edilen elektronik bilgi varlıkların korunması, şirket bünyesinde tutulan kişisel verilerin kanun kapsamında işlenmesi, saklanması, korunması, gizliliğinin ve bütünlüğünün bozulmaması için kullandığı bilgi güvenliği süreçlerini kapsar.

2.1. İç Kapsam

İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler;

2.1.1. Şirket Üst Yönetimi bünyesinde bulunan kapsam dahilindeki departmanlar;, Mali ve İdari İşler, Satınalma, Finans, Bilgi İşlem, Kurumsal İletişim ve İş Geliştirme, İnsan Kaynakları, Kalite, İhracat, İthalat, Lojistik, Hukuk, İç Denetim, Satış, Pazarlama

2.1.2. Genel Yönetim Organizasyon Şemasında belirtilmiş roller ve görev tanımlarındaki sorumluluklar.

2.1.3. Yerine getirilecek politikalar, prosedürler, hedefler ve stratejiler;

- Bilgi Güvenliği Yönetim Sistemi Politikası,
- Tüm Bilgi Güvenliği yönetim sistemleri talimatları ,
- Yönetimce belirlenmiş yıllık Bilgi Güvenliği yönetim sistemleri hedefleri,
- Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara,

zaman, kişiler, süreçler, sistemler ve teknolojiler),

- Bilgi Güvenliği Yönetim Sisteminin kurulması, işletilmesi ve sürdürülmesi için yönetim tarafından atanan Yönetim Temsilcileri ve Bilgi Güvenliği Yönetim Sistemi ekibi,

- İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri, kuruluşun kültürü, kuruluş tarafından uyarlanan standartlar, kılavuzlar ve modeller, sözleşmeye ilişkin ilişkilerin; biçim ve genişliğini kapsamaktadır.

3. Tanımlar

a- BGYS : Bilgi Güvenliği Yönetim Sistemi.
b- Envanter : Firma için önemli olan her türlü bilgi varlığı.
c- Üst Yönetim : Şirket Üst Yönetimidir.
d- Know-How : Bir şeyi yapabilme yetkinliğidir.

e- Bilgi Güvenliği: Bilgi, tüm diğer kurumsal ve ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun şekilde korunması gereken bir varlıktır. Şirket içerisinde, know-how, süreç, formül, teknik ve yöntem, müşteri kayıtları, pazarlama ve satış bilgileri, personel bilgileri, ticari, sınai ve teknolojik bilgiler ve sırlar GİZLİ BİLGİ olarak kabul edilir.

f- 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)

g- 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)

h- 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. (Örnek: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şaselerinde yedekli güç kaynağı kullanımı - UPS). Bu politikada "Erişilebilirlik" olarak kullanılacaktır.

i- Bilgi Varlığı : Şirket'in 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. Sorumluluklar

Revizyon Nedeni:	Hazırlayan	Kontrol Eden	Onaylayan
	Bilgi İşlem Ekibi	Bilgi İşlem Sorumlusu / Hukuk Birimi	Genel Müdür

Sorumluluk ve yetkileri belirlenmiş görevlerin nitelik ve yeterlilikleri görev tanımlarında tanımlanmıştır. Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Bilgi İşlem Ekibi ve Yönetim Temsilcisi sorumludur. BGYS Ekibi ve Yönetim Temsilcileri Üst Yönetim tarafından atanmıştır. Kapsam içindeki departmanlardan BGYS temsilcileri belirlenmiştir. BGYS ekip üyesi olarak isim bazında atamaları yapılmıştır.

Şirket 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.

Üst kademelerden başlayan ve uygulanan anlayış, firmanın en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden tüm yöneticiler yazılı ya da sözlü olarak güvenlik talimatlarına uymaları, güvenlik konularındaki çalışmalara katılmaları yönünde çalışanlarına destek olurlar.

5. Bilgi Güvenliği Hedefleri

Bilgi Güvenliği Politikası, Şirket çalışanlarına firmanın güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini arttırmak ve bu şekilde şirketin temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, güvenilirliğini ve imajını korumak ve üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunlukları sağlamak amacıyla firmanın tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarının korunmasını hedefler.

6. Risk Yönetim Çerçevesi

Firmanın 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 Bilgi işlem birimi sorumludur. Bu hususlar Kişisel Verim İşleme Envanteri ve risk değerlendirme talimatında detaylı olarak açıklanır.

7. Bilgi Güvenliği GenelEsasları

Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, Şirket çalışanları ve 3. taraflar bu politika ve prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

7.1. Bu kural ve politikalar, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.

7.2. Şirket tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça şirkete aittir.

Revizyon Nedeni:	Hazırlayan	Kontrol Eden	Onaylayan
	Bilgi İşlem Ekibi	Bilgi İşlem Sorumlusu / Hukuk Birimi	Genel Müdür

7.3. Çalışanlar, danışmanlık, hizmet alımı (Güvenlik, servis, yemek, temizlik firması vb.), Tedarikçi ve Stajyer ile gizlilik anlaşmaları yapılır.

7.4. İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.

7.5. Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut şirket çalışanlarına ve yeni işe başlayan çalışanlara verilir.

7.6. Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemleralınır.

7.7. Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.

7.8. Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.

7.9. Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.

7.10. Firmaya ait bilgi varlıkları için firma içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.

7.11. Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.

7.12. 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.

7.13. Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.

7.14. Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.

7.15. Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.

7.16. 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. Politikanın İhlali ve Yaptırımlar

Revizyon Nedeni:	Hazırlayan	Kontrol Eden	Onaylayan
	Bilgi İşlem Ekibi	Bilgi İşlem Sorumlusu / Hukuk Birimi	Genel Müdür

Bilgi Güvenliği Politikasına ve Standartlarına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar için İşyeri Disiplin Yönetmeliği ve KVKK nun ilgili uyarınca gerekli yaptırımlar uygulanmaktadır.

9. DİĞER HUSUSLAR

KVKK ve ilgili diğer mevzuat hükümleri ile işbu Politika arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili diğer mevzuat hükümleri uygulanacaktır.

Politika'da değişiklik olması durumunda, Politika'nın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir. Güncelleme tablosu "Doküman Künyesi" nde yer almaktadır.

10. Güncelleme

İşbu Politika yılda bir defa, ilgili Holding Hukuk Müşavirliği tarafından gözden geçirilir ve güncellenir.

11. Yürürlük

Şirket tarafından hazırlanan işbu Politika 16/11/2020 tarihinde yürürlüğe girmiştir.

12. Yürütme

Dökümanın yürütme sorumluluğunu, Bilgi İşlem Sorumlusuna ve Hukuk Müşavirliği Bölümü'ne aittir.

13. Dağıtım

Politika, şirket internet sitesinde ve Şirket intranetinde yayınlanarak, üçüncü taraflara ve Şirket çalışanlarına duyurulur.

Revizyon Nedeni:	Hazırlayan	Kontrol Eden	Onaylayan
	Bilgi İşlem Ekibi	Bilgi İşlem Sorumlusu / Hukuk Birimi	Genel Müdür