## BGYS POLİTİKASI

BGYS politikası, **DESA DERİ SAN. VE TİC. A.Ş.** bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır. Bu politikada tüm bölümleri ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır.

## 1. AMAÇ:

Bu politikanın amacı; temel bilgi güvenliği prensiplerini tanımlamak ve bu prensiplere üst yönetimin verdiği desteği ifade etmektir.

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat kurum açısından en önemli varlıklardan biridir. Bilgi güvenliği yönetim sistemimiz TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardına uygun olarak kurulmuş ve bu standardın gerekliliklerini karşılayacak şekilde PUKÖ (Planla, Uygula, Kontrol Et, Önlem Al) sürekli iyileştirme döngüsü çerçevesinde bir süreç olarak uygulanmaktadır.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımızın genel özeti bu politikada verilmektedir. Uygulama detay bilgileri için sistem dokümantasyonuna, ilgili prosedürlere, talimatlara, planlara ve formlara bakılmalıdır. Bu politika bilgi güvenliği politikası ve detaylı kullanım politikalarını da kapsayan bir üst dokümandır.

Yönetim tarafından onaylanmış ve yayınlanmıştır. Yönetim tarafından düzenli olarak gözden geçirilmektedir.

| HAZIRLAYAN | ONAYLAYAN |
|---|---|
| | |

## 2. KAPSAM:

Bu politikanın kapsamı tüm organizasyon ve bilgi varlıklarıdır.

## 3. SORUMLULUKLAR:

## 4.

### 4.1. Genel Müdür

Politikanın şirketin bilgi güvenliği ihtiyaçlarını karşılar nitelikte bulunmasından ve politikanın uygulanması için gerekli kaynak ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya politikada değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur.

### 4.2. BGYS Temsilcisi

Genel Müdür tarafından görevlendirilen BGYS Temsilcisi, Bilgi Güvenliği Politikasının şirket ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından sorumludur.

### 4.3. Tüm Personel

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

## ROL VE SORUMLULUKLAR

Bu bölümde DESA DERİ SAN. VE TİC. A.Ş. için bilgi güvenliği sorumlulukları belirtilmektedir.

| Taraflar | Sorumluluklar |
|---|---|
| **BGYS Temsilcisi Yönetim** | *Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesi için gerekli kaynak ve sorumluluk tahsislerini gerçekleştirmek,<br>*BGYS altyapısını desteklemek ve işleyişini devam ettirmek,<br>*Çalışanların BGYS hakkında bilgilenmelerini sağlayacak mekanizmaların işletilmesini sağlamak,<br>*Çalışanların bilgi güvenliğine ilişkin olarak karşılaşabileceği riskleri anlaması ve tanıması için eğitici yöntemlerin kullanımını sağlamak,<br>*Bilgi güvenliğini sağlamaya yönelik olarak tespit edilen ihtiyaçların karşılanmasını planlamak ve sağlamak,<br>*Güvenlik Politikasını onaylamak ve firma içinde uygulanmasını sağlamak,<br>*BGYS kapsamlı dokümanları onaylamak,<br>*BGYS kapsamlı Risk analizi sonucunda ortaya çıkan artık riskleri onaylamak.<br>*Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesini sağlamak,<br>*Yönetim Gözden Geçirme toplantılarını koordine etmek, BGYS dokümanlarının revizyonunu ve kontrolünü yapmak,<br>*BGYS kapsamlı dokümanları onaylamak,<br>*Çalışanların bilgi güvenliği farkındalık eğitimlerinin koordine edilmesi ve eğitim etkinliklerinin değerlendirilmesi,<br>*Risk analizi sonuçlarını değerlendirmek, kontrollerin belirlenmesi ve uygulanmasını koordine etmek,<br>*Bilgi Güvenliği İhlal olaylarını değerlendirmek ve takibini yapmak,<br>*Bilgi Güvenliği'ne ilişkin Düzeltici ve Önleyici faaliyetleri takip etmek ve kayıtları onaylamak, |

| | |
|---|---|
| | *Bilgi Güvenliği Politikası'nı belli aralıklarla gözden geçirmek ve BGYS Yönetim Temsilcisi'nin onaylamasını sağlamak. |
| **Birim Müdürleri** | *Bilgi Güvenliği Politikası'nı uygulamak ve çalışanlarının esaslara bağlılıklarını sağlamak,<br>*Üçüncü taraf bilgi sistemleri kullanıcılarının politikadan haberdar olmasını sağlamak,<br>*Fark ettiği veya kendisine iletilen bilgi sistemleri ile ilgili güvenlik ihlal olaylarını BGYS Yöneticisine bildirmek,<br>*Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncellemelerde bulunmak,<br>*Faaliyet gösterdikleri konularla ilgili otoritelerle iletişimi sağlamak. |
| **Tüm çalışanlar** | *Bilgi Güvenliği Politikasını bilmek ve uymak,<br>*BGYS kapsamında belirlenen uyulması gereken davranışlara riayet etmek,<br>*BGYS'nin sağlıklı işlemesi için gerekli görülen önerileri ilgilisine iletmek ve sistemin iyileştirilmesine katkıda bulunmak,<br>*Fark ettiği bilgi sistemleri ile ilgili güvenlik ihlal olaylarını Birim |

| | |
|---|---|
| | Müdürüne bildirmek,<br>*Bilgi Güvenliği Farkındalık eğitimlerine katılmak. |
| **3.Taraflar-Tedarikçiler** | *Bilgi Güvenliği Politikasını bilmek ve uymak,<br>*BGYS kapsamında belirlenen uyulması gereken davranışlara riayet etmek, |

## 5. TANIMLAR

| | | |
|---|---|---|
| **BGYS** | **:** | Bilgi Güvenliği Yönetim Sistemi |
| **Risk Yönetimi** | **:** | Bilgi güvenliği risklerinin analizi, değerlendirilmesi, işlenmesi ve sürekli iyileştirilmesi amacıyla yürütülen yönetimsel faaliyetler. |
| **Risk Analizi** | **:** | Tehdit ve iş etkisinin çarpımı olan risk puanının bulunması amacıyla her bir bilgi varlığı için zayıflıkların, tehditlerin, iş etkilerinin bulunması ve hesaplanması çalışması. |
| **Risk Değerlendirme** | **:** | Risk analizi sonucunda bulunan değerlerin yorumlanması ve derecelendirilmesi. |
| **Risk İşleme** | **:** | Risk değerlendirme sonuçlarına bağlı olarak kaçınma, kabul, kontrol, transfer seçeneklerinden birinin seçilmesi ve uygulama planı. |
| **Artık Risk** | **:** | Risklerin işlemeden sonra kalan miktarıdır. |
| **Risk Derecelendirmesi** | **:** | Riskin önemini tayin etmek amacıyla tahmin edilen riskin, verilen risk kriterleri ile karşılaştırılması sürecidir. |

| HAZIRLAYAN | ONAYLAYAN |
|---|---|
| | |

| | | |
|---|---|---|
| **Gizlilik** | **:** | Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. |
| **Bütünlük** | **:** | Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. |
| **Erişilebilirlik** | **:** | Bilginin ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. |
| **Riskin Kabulü/Kabul edilebilir Risk** | **:** | Bir riski kabul etme kararı. Bir riskin zararını (negatif sonuçlarını) kabullenme. |
| **Bilgi Güvenliği** | **:** | Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar. |
| **Bilgi güvenliği ihlal olayı** | **:** | İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı. |
| **Bilgi güvenliği yönetim sistemi (BGYS)** | **:** | Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir. |
| **Uygulanabilirlik Bildirgesi (SOA-Statement of Applicability)** | **:** | Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirgedir. Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır. |

| | | |
|---|---|---|
| **Etki** | **:** | İş hedeflerinin başarısını etkileyen değişim. |
| **Bilgi Güvenliği Riski** | **:** | Açıklıklardan fayda sağlamak suretiyle kuruluşa zarar verebilecek varlık ya da varlık gruplarının potansiyel tehdididir. Bir olayın ve sonucunun olasılığının kombinasyon koşulları olarak ölçülür. |
| **Riskten kaçınma** | **:** | Riski oluşturan durumdan kaçınma kararıdır. |
| **Risk iletimi** | **:** | Karar verici veya diğer ortaklar arasında risk hakkındaki bilgiyi paylaşım ya da değişimdir. |
| **Riski belirleme** | **:** | Riski oluşturan öğelerin ortaya çıkartılması, tasnif edilmesi ve özelliklerinin belirlenmesini içeren süreçtir. |
| **Riski transfer etme** | **:** | Bir riskin kayıplarını diğer paydaşlarla paylaşma. (Sigorta yaptırma gibi) |

## 6. UYGULAMA

**BGYS Politikası**
**Genel Esaslar**

- ✓ Kurumsal bilgileri, personel özlük bilgilerini, müşteri verilerini (finansal veriler, kişi bilgileri...) değerli ve kritik kabul etmekte ve bilgi güvenliği ile ilgili yasaların gerektirdiği zorunlulukları yerine getirmeyi,
- ✓ Kurumsal faaliyetlerimizin gerçekleşmesinde kullanılan bilişim hizmetlerinin kesintisiz devam etmesi, kişisel ve özel verilere erişimin sadece yetkili kişilerce erişilebilmesi amacıyla gerekli altyapıyı sağlamayı ve gerekli güvenlik tedbirlerini almayı,
- ✓ Bilgi güvenliği yönetim sistemimizin ISO/IEC 27001 standardının gereklerini yerine getirecek şekilde dokümante etmeyi ve sürekli iyileştirmeyi,
- ✓ Bilgi güvenliği ile ilgili tüm yasal mevzuat ve sözleşmelere uymayı,
- ✓ Bilgi varlıklarına yönelik riskleri sistematik olarak yönetmeyi,
- ✓ Bilgi güvenliği farkındalığını artırmak amacıyla teknik ve davranışsal yetkinlikleri geliştirecek eğitimleri gerçekleştirmeyi,

## 7. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında **Disiplin Prosedürü** hükümleri uygulanır.

| HAZIRLAYAN | ONAYLAYAN |
|---|---|
| | |