

ZORLU GRAND HOTEL İŞLETMELERİ ANONİM ŞİRKETİ BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ VE KAPSAM	1
2. TANIMLAR.....	1
3. BİLGİ GÜVENLİĞİ İHTİYACI.....	2
4. BİLGİ GÜVENLİĞİ AMAÇLARI	2
5. BİLGİ GÜVENLİĞİ POLİTİKASI	2
6- ÜST YÖNETİMİN BİLGİ GÜVENLİĞİ LİDERLİĞİ.....	3
7. GÖREV VE SORUMLULUKLAR	3
8- POLİTİKANIN İHLALİ VE YAPTIRIMLAR	4
9- UYUMLULUK	4
10- GÖZDEN GEÇİRME VE REVİZYON	4

1. AMAÇ VE KAPSAM

Bu politikanın amacı “Şirket” olarak anılan Zorlu Grand Hotel’de yürütülen BGYS kapsamında bilgi güvenliğini sağlamak için uygulanacak temel politikaları ortaya koymak, bilgi güvenliği hedeflerinin yönetimi ve bilgi güvenliğinin sürekli iyileştirilmesi için genel bir çerçeve oluşturmak ve üst yönetimin bilgi güvenliğindeki liderlik rolü ve sisteme bağlılığını açık olarak ifade etmektir.

2. TANIMLAR

Şirket / Zorlu Grand Hotel : Zorlu Grand Hotel İşl. A.Ş.

Paydaş: Şirket kapsamında yürütülen faaliyetlerden olumlu veya olumsuz bir şekilde doğrudan veya dolaylı bir şekilde etkilenecek kurumlar, firmalar veya kişilerdir.

Üçüncü Taraflar: Şirkete sözleşme ile hizmet sağlayan tüzel kişiler ve personelleridir.

Personel: Şirkette çalışan sözleşmeli/toplu iş sözleşmeli personeldir.

Bilgi Güvenliği: Şirket varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunmasıdır.

BGYS: Bilgi Güvenliği Yönetim Sistemi.

Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olmasıdır.

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmesine karşı korunması ve değiştirildiğinde farkına varılmasıdır.

Erişilebilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an erişilebilir olması

Bilgi: Kurumun varlığını sürdürebilmesi amacıyla yürüttüğü operasyonlar için gerekli ve kurum için değerli olan verilerdir.

Bilgi Varlığı / Varlık: Bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken bilgileri içeren veya bu bilgilerin işlenmesine yardımcı olan tüm unsurlardır.

3. BİLGİ GÜVENLİĞİ İHTİYACI

Şirketimiz bilgi güvenliğine yönelik içeriden ve dışarıdan gelebilecek saldırılara karşı korunmak, şirketimiz için değerli bilgileri korumak ve şirketimizde gerçekleştirilen faaliyetlerde güvenliği sağlamak ancak bilgi güvenliği uygulamaları ile mümkün olabilir.

Şirketimiz bilgi ve bilgi varlıklarına yönelik risklerin belirlenmesi ve işlenmesi amaçlamaktadır. Ayrıca, bilgi güvenliği konusunda şirket içerisindeki farkındalığı arttırmak ve bilgi güvenliği ile süreçlerin hayata geçirilmesini sağlamayı hedeflemektedir. Bunlarla birlikte şirketimizin de içinde yer aldığı sektördeki yasal zorunluluklara uyum ve benzer sektörlere yönelik tehditlerin çoğalması bilgi güvenliğine olan ihtiyacı artırmıştır. Bu sebeplerle şirket genelinde yürütülecek bir Bilgi Güvenliği Yönetim Sistemi kurulmuştur.

4. BİLGİ GÜVENLİĞİ AMAÇLARI

BGYS, Şirketin sahip olduğu bilgi, bilgi varlıkları ve sunduğu hizmetlerin güvenliğini aşağıdaki prensipler doğrultusunda sağlamayı amaçlamaktadır:

- Personel, paydaş ve üçüncü kişilerin bilgi güvenliği farkındalıklarını arttırmak.
- Bilgi varlıklarının güvenliği için etkin teknik güvenlik kontrollerini uygulamak.
- Riskleri en aza indirerek Şirketin güvenliğini, güvenilirliğini ve imajını korumak.
- Şirket tarafından üretilen, kullanılan, geliştirilen bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak ve korumak.
- Şirketin tabi olduğu mevzuat, yasa ve yönetmeliklerin gerekliliklerinin karşılanmasını sağlamak.
- Paydaşlar ve üçüncü kişiler ile yapılan sözleşmelere uyumu sağlamak.

Şirketimiz yukarıda belirtilen bilgi güvenliği amaçlarını sağlamak için BGYS hedeflerini belirlemekte, bu hedeflere yönelik planlamaları yapmakta ve hedeflerin başarımını takip etmektedir. Bu hedefler üst yönetim tarafından belirlenir ve bilgi teknolojileri müdürlüğü tarafından planlanarak takip edilir.

5. BİLGİ GÜVENLİĞİ POLİTİKASI

Şirketimiz, BGYS amaç ve hedeflerini sağlamak amacıyla, aşağıda özetlenen Bilgi Güvenliği Politikalarını tüm şirket genelinde uygulamaktadır.

- Şirketimiz bilgileri kullanım amaçlarına uygun bir şekilde gizlilik açısından sınıflandırılır, bu sınıflandırmalara göre erişim politikasına uygun olarak, yetkisiz erişime karşı korunur ve yetkisiz kişilere kasten veya dikkatsizlik sonucu verilmez.
- Şirketimiz bilgilerinin doğruluğu erişim politikasına uygun olarak, yetkisiz değişikliklere karşı korunur.
- Şirketimiz bilgileri, gereksinim duyulduğunda yetkili kullanıcıların erişimine hazır bulundurulur.
- Şirketimizde görev alan üçüncü taraflar şirketimiz bilgi güvenliği politikaları hakkında bilgilendirilir ve bu politikalara uygun davranırlar.
- Şirketimizin tabi olduğu mevzuat, yasa ve yönetmeliklerin şartları denetim ve uyum politikası'na uygun olarak yerine getirilir.

- Şirketimizin güvenilir imajı korunur.
- Paydaşlar ve üçüncü kişilerle yapılan sözleşmelere uygun hareket edilir.
- Tüm birimler, bilgi güvenliği ile ilgili tüm prosedür ve politikalara uygun hareket eder.
- Tüm personele bilgi güvenliği farkındalığı eğitimleri verilir.
- Tüm personel, haberdar oldukları bilgi güvenliği olaylarını bağlı bulunduğu departman yöneticisine, KVK Kurul üyelerine ve üst yönetime bildirmekle yükümlüdürler.

6. ÜST YÖNETİMİN BİLGİ GÜVENLİĞİ LİDERLİĞİ

BGYS'nin kurulması ve işletilmesi amacıyla Bilgi Teknolojileri Müdürlüğü ve KVK Kurulu ekibi atanmış sorumluluklar da tanımlanmıştır. BGYS'nin kurulması ve işletimi için gerekli tüm kaynaklar üst yönetim tarafından sağlanmaktadır.

BGYS kapsamında oluşturulan politika ve prosedürler şirketimizde bilgi güvenliğinin sağlanması için uyulacak kuralları ve işletilecek süreçleri ortaya koymaktadır. Tüm personelin bu politika ve prosedürlere uyması ve bu doğrultuda hareket etmeleri gerekmektedir. Bilgi güvenliği politikaları ve süreçleri, şirketimizde yürütülen diğer faaliyetlerle aynı öneme sahip olup bunlarla bütünleşik olarak yürütülecektir. Şirketimizin tüm operasyonlarını gerçekleştiren birimlerin yönetiminden sorumlu müdürlerimiz BGYS politika ve prosedürlerinin kendi birimlerinde uygulanmasını sağlamaktan sorumludur.

BGYS'nin geliştirilmesi ve iyileştirilmesi Bilgi Teknolojileri Müdürlüğü ve KVK Kurul üyelerinin olduğu kadar tüm personelin sorumluluğundadır. Herkesin bu sistemin iyileştirilmesine katkı sağlayacak önerilerde bulunması beklenmektedir.

Bu şartlara, BGYS politika ve prosedürlerine uyulmaması durumunda aşağıda yer alan "Politikanın İhlali ve Yaptırımlar" maddesine göre yaptırımlar uygulanacaktır.

7. GÖREVLER VE SORUMLULUKLAR

Şirketimizde bilgi teknolojileri altyapısının kurulması ve yönetilmesinden Bilgi Teknolojileri Müdürlüğü sorumludur. Buna bağlı olarak, Şirketimizin bu altyapı üzerindeki bilgi güvenliği uygulamaları da yine Bilgi Teknolojileri Müdürlüğü tarafından yürütülmektedir.

Şirket üst yönetimi, bu politikayı oluşturur, uygulanmasını sağlar ve gözden geçirir. Ek olarak üst yönetim BGYS'nin kurulmasından, işletilmesinden, altyapısını desteklemekten, işleyişini izlemek ve denetlemekten de sorumludur. Üst yönetim, bu amaçla Bilgi Güvenliği Yöneticisi ve ekibini atamıştır. Bilgi Güvenliği Yöneticisi ve ekibi, BGYS'nin işleyişini izler, sürekliliğini sağlar ve üst yönetim adına yukarıdaki çalışmalarını yürütür.

Bilgi güvenliği ile ilgili tüm personeli ilgilendiren sorumluluklar aşağıda tanımlanmıştır:

- Tüm Şirket ve üçüncü taraf personeli bilgi güvenliği politika ve prosedürlerini bilmek, bu kural ve esaslara uygun davranmaktan sorumludur.
- Tüm Şirket ve üçüncü taraf personeli güvenlik olaylarını, fark edilen güvenlik açıklıklarını ve güvenlik politikaları ihlallerini en kısa sürede Bilgi Güvenliği Yöneticisine, KVK Kurul üyelerine veya Departman Yöneticisine bildirmekten sorumludur.
- Şirket bilgi varlıklarının sahipleri, varlıkların gizlilik, bütünlük, erişilebilirliğinin korunmasından sorumludur.
- Şirket bilgi kaynakları izinsiz olarak paydaş ve üçüncü kişiler ile paylaşamaz.
- Tüm personel bilgi güvenliği farkındalığını arttırmak amacıyla yapılan farkındalık eğitimlerine katılmalıdır.

8. POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Şirket bilgi güvenliği politikalarına ve prosedürlerine uymayan veya ihlal eden personeller için disiplin yönetmeliğinde bulunan tüm maddeler geçerlidir.

9. UYUMLULUK

Tüm personel ve üçüncü taraf personeli bu politikaya uygun davranmaktan sorumludur. Bilgi Güvenliği Yöneticisi ve KVK Kurul üyeleri de bu politikanın uygulanmasından, uygulamanın denetlenmesinden ve politika dokümanının güncel tutulmasından sorumludur.

10. GÖZDEN GEÇİRME VE REVİZYON

Bilgi Güvenliği Politikası, Bilgi Güvenliği Yöneticisi ve KVK Kurul üyeleri tarafından periyodik olarak yılda bir kez gözden geçirilir. Bilgi güvenliği ile ilgili diğer politika ve prosedürlerdeki değişiklikler politikanın gözden geçirilmesini gerektirebilir. Gözden geçirilen ve güncellenen politika üst yönetim tarafından onaylanır ve ilgili taraflara iletilir. Onaylanan politika ortak klasörde yayınlanır.