Bilgi Güvenliği Politikası

EYS.P0.01 Rev:00 Yayın Tarihi:02.01.2023 Rev. Tarihi: --

İÇİNDEKİLER

Hazırlayan	Onaylayan
Yönetim Temsilcisi	**Genel Müdür**

1. Giriş

TS ISO/IEC 27001:2013 BGYS kapsamında oluşturulan Bilgi Güvenliği Politikası, kurum içerisinde yürütülen bilgi güvenliği yönetim sistemine yönelik çalışmalarının amacını, kapsamını, içeriğini, kullanılan yöntemleri, katılımcıları, görev ve sorumlulukları, uyulması gereken kuralları içerecek bir rehber niteliğinde hazırlanmıştır. Bu politika dokümanı, bilgi güvenliği politikası ve detaylı kullanım politikalarını da kapsayan bir üst dokümandır.
Yönetim tarafından onaylanmış ve yayınlanmıştır. Yönetim tarafından düzenli olarak gözden geçirilmektedir.

1.1. Amaç

Şirketimiz' in gerçekleştirdiği faaliyetlerle ilgili sahip olduğu bilginin güvenliğinin sağlanması, geliştirilmesi ve artırılması amacıyla TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi uyum çalışmaları başlatılmıştır. Bu çalışmaların bir başka önemli özelliği kurulacak sistemin devamlılığını ve sürekli iyileştirilmesini sağlamaktır.

Bilgi güvenliği, sadece bilgi teknolojileri çalışanlarının sorumluluğunda, değil **Şirketimiz**' in tüm çalışanlarının katılımı ve riayeti ile başarılabilecek bir iştir. Bununla birlikte sadece bilgi teknolojileri ile ilgili teknik önlemlerin alınmasından, süreçlerin çalıştırılmasından ibaret de değildir. Bu sistem alt katmanlarda fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, üst katmanda iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine kadar birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi, uygulanması ve sürekli ölçülmesini içermektedir. Uygulama detay bilgileri sistem dokümantasyonu, ilgili prosedürler, rehberler, planlar ve raporlarda yer almaktadır.

Şirketimiz Çalışanları, Müşterileri, Finansal, Tedarik ve Son Kullanıcı datalarının korunması;

1.2. Kapsam

Şirketimiz Yönetim Sistemi ve Çevresel Kapsamı **Kuruluşun Kapsamı** dokümanında tanımlanmıştır.

1.3. İlgili Taraflar

Kapsam dahilinde gerçekleştirilen faaliyetlerde; faaliyetle ilgili yasal ve düzenleyici yükümlülüklerden dolayı **Şirketimiz'** de kurulan BGYS' nin ilgili **tarafları İlgili Tarafların İhtiyaç ve Beklentileri** dokümanında listelenmiştir.

2. Bilgi Güvenliği Hedefleri ve Prensipleri

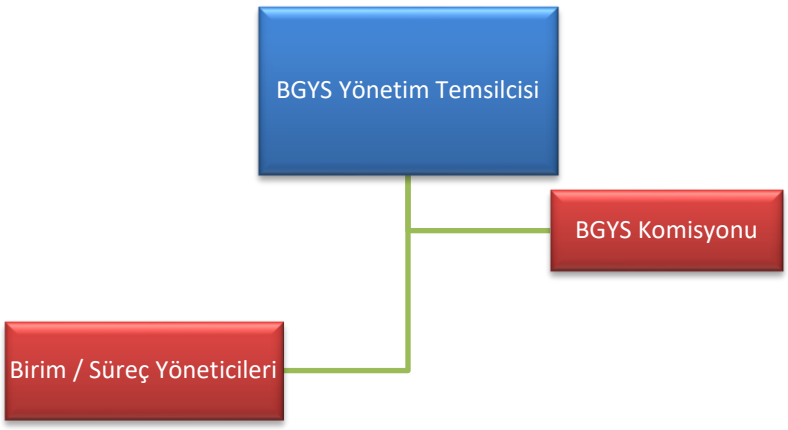
Bilgi güvenliği yönetimi kapsamına alınan varlıklar ve bunlarla ilgili tüm süreçlerde; **G**izlilik, **B**ütünlük ve **E**rişilebilirlik prensiplerine uyacak önlemler almak amacıyla çeşitli faaliyetler yürütülmektedir. Bu faaliyetler **Varlık – Kaynak Envanter Planı'**nda yer almaktadır. Şirketimiz Bilgi Güvenliği Yönetim Sistemi, gerçekleştireceği Risk Yönetimi ile her bir varlık için risk seviyesini, kabul edilebilir risk seviyesinin altında

tutmayı hedeflemektedir. Risk yönetimi ve kontrollerin uygulanması sürekli bir faaliyettir. Bu nedenle kabul edilebilir risk seviyesinin altına inecek riskler için de iyileştirmeler yapılması hedeflenmektedir.

Şirketimiz BGYS ile aşağıda belirlenen hedefleri gerçekleştirmeyi amaçlamıştır.

BGYS Hedefi	Performans Kriteri
1. Tüm çalışanların bilgi güvenliği farkındalığını artırmak.	Yıllık en az 1 BGYS eğitim sayısı
2. Başarılı yedekleme oranını belli seviyede tutmak.	Yıllık en az %95 başarılı yedekleme sayısı
3. Başarılı yedekten dönme oranını belli seviyede tutmak.	Yıllık %95 başarılı yedekten dönüş sayısı
4. Tüm sunucu ve kullanıcı sistemlerinde kurulmuş anti virüs oranını belli seviyede tutmak.	%100 AV kurulmuş sistem oranı
5. Ana internet bağlantısında SLA hedefini yakalamak.	Yıllık %99 up-time
7. BG Komisyonu toplantı sayısını belli seviyede tutmak.	Yıllık en az 3 toplantı
8. İç tetkik sayısını belli seviyede tutmak.	Yıllık en az 1 iç tetkik
9. Yönetimin gözden geçirme sayısını belli seviyede tutmak.	Yıllık en az 1 gözden geçirme
10. Risk işleme planı gözden geçirme sayısını belli seviyede tutmak.	Yıllık en az 1 gözden geçirme

3. Bilgi Güvenliği Organizasyonu ve Altyapısı



Hazırlayan	Onaylayan
Yönetim Temsilcisi	**Genel Müdür**

3.1. BGYS Görev Tanımları ve Yetkileri

Görev **: BGYS Sponsoru – Üst Yönetim**
Yetki ve Sorumluluklar **:** BGYS' nin kurulması ve çalıştırılması için gerekli kaynakları sağlamak
Birimin sunduğu kontrol seçimlerine onay vermek
Yatırım ve değişimler için onay vermek
Düzenli BGYS Gözden Geçirme toplantılarına başkanlık etmek
Kurum çalışanlarının katılımı için teşvik edici faaliyetler düzenlemek
BGYS yöneticisi ile BGYS birimini atamak ve yetkilendirmek
BGYS risk kabul kriterlerini belirlemek, kabul edilecek riskleri onaylamak
BGYS Komisyonuna başkanlık etmek veya Yönetim Temsilcisine vekalet vermek.

Görev **: Yönetim Temsilcisi**
Yetki ve Sorumluluklar **:** BGYS hazırlık, işletme, süreklilik ve iyileştirme faaliyetlerini yönetmek
BGYS politikası ve prosedürlerinin hazırlamak, gerektiğinde revize etmek
Kayıt sisteminin kurulması ile BGYS' nin gerektirdiği kayıtların tutulmasını sağlamak
Risk yönetimi faaliyetlerinin sürekli ve düzgün yapılmasını sağlamak
Kontrollerin etkinliğini ölçmek
Tehdit ve zayıflık veri tabanını güncel tutup değişen riski yönetmek
Tetkik ve İç tetkik planlama ve uygulama faaliyetlerini yönetmek
Değişim ve konfigürasyon yönetimi faaliyetlerini sağlamak
Acil durum müdahale ekibinin başında bulunmak
YGG toplantılarını organize etmek
Üst yönetimi EYS kapsamında yapılan çalışmalarda bilgilendirmek

Yetkinlikler : Üniversite Mezunu
Orta düzey İngilizce bilgisi
Baş denetçi eğitimi almış olması
Minimum 2 yıl mesleki denetim
BGYS Sistemi kurmuş veya yönetmiş olması

Görev Yetki ve Sorumluluklar **: BGYS Komisyonu**
: BGYS' nin kurulması ve çalışmaların, TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı hükümleri çerçevesince yürütülmesi hususunda kararlar almak.

Yetkinlikler : Komisyon Başkanı Üniversite Mezunu
Orta düzey İngilizce bilgisi
Minimum 2 yıl mesleki denetim
Ekip çalışmasına yatkın, Düzenli
BGYS ile ilgili temel ve dokümantasyon eğitimi almış olması

Görev Yetki ve Sorumluluklar	**: Birim / Süreç Yöneticileri** : BGYS iç tetkiklerine katılmak ve görev almak BGYS kontrol uygulamalarını hayata geçirmek ve izlemek Acil durum eylem planlarında üzerine düşen görevleri yapmak Planlama ve raporlama için BG yöneticisine yardımcı olmak
Yetkinlikler	: Üniversite Mezunu Orta düzey İngilizce bilgisi Minimum 2 yıl mesleki denetim Ekip çalışmasına yatkın, Düzenli Kalite ve BGYS ile ilgili temel ve dokümantasyon eğitimi almış olması

3.2. BGYS Uygulamalarına Katılım

Şirketimiz çalışanlarının tamamı bu politikada belirtilen şartlara ve kurallara uymak zorundadır. Bilgi güvenliği takımının BGYS ile ilgili görevlerini yerine getirmesinde yardımcı olmalıdır. Her çalışan, yönetimce yayınlanan bu politikada belirtilen amaçlara ulaşmak için yürütülen risk yönetimi çalışmalarına ve bilgi güvenliği rehberinde belirtilen kurallara uymakla sorumludur. Talimatlara ve kontrollere uymayanlara aşağıda belirtilen disiplin sürecine göre işlem yapılacaktır.
Her çalışan, kendisinin sorumluluğunda ve yönetiminde olan bilgi varlıklarının kontrolü ile gizliliğinden sorumludur. Kurumumuzun seçtiği risk yönetimi metodolojisi çerçevesinde, bu varlıklara yönelik olarak yapılacak gerekli analizlere katılmak ve kontrolleri uygulamak, her çalışanın görevleri arasındadır.
Çalışanlar, uygulanan kontrollerin yeterliliğini ve verimliliğini izlemek ile güvenlik ihlal olaylarını veya ihlale yol açabilecek tehdit ve zayıflıkları, aşağıda belirtilen ihlal olayı prosedürüne göre, gecikmeden raporlamak zorundadır.
Bilgi güvenliği yöneticilerinin bilgisi olmadan, bilgi varlıkları ile ilgili donanımsal, yazılımsal veya fiziksel herhangi bir değişiklik yapılmamalıdır. Yapılması gereken değişiklikler ile ilgili BGYS takımı yöneticisine mutlaka haber verilmeli ve değişiklik için aşağıda belirtilen değişim yönetimi prosedürüne uygun kayıt tutulmalıdır. Bunun yanında konfigürasyon yönetimi prosedüründe belirtilen varlık özelliklerinin değiştirilmesi ile ilgili kayıtlarda mutlaka oluşturulmalıdır.

3.3. BGYS YGG Toplantısı

Yönetimin Gözden Geçirme Toplantısı; üst yönetim ile BGYS Komisyonu üyelerinin yer aldığı, BGYS'nin uygunluğunun, verimliliğinin, risk yönetiminin işlevselliğinin, tetkik sonuçlarının, düzeltici ve iyileştirici faaliyetlerin ele alınıp değerlendirildiği yılda en az bir defa yapılan toplantıdır. BGYS Toplantısı YGG toplantısını müteakiben veya YGG toplantısı ile birlikte de yapılabilir. Bu toplantıda yönetim, risk kabul kriterlerini ve ilgili kaynak ihtiyaçlarını değerlendirir. Çalışmaların, risk değerlendirme ve işleme faaliyetlerinin verimliliği de bu toplantıda incelenir.

Bu toplantılarda kullanılan girdi ve çıktılar, standarda uygun olarak **Toplantı Tutanağı Formu** kullanılarak kayıt altına alınmaktadır.

Hazırlayan	Onaylayan
Yönetim Temsilcisi	**Genel Müdür**

4. Risk Değerlendirme ve Risk İzleme

Şirketimiz bünyesinde yürütülmekte olan ISO 9001:2015 Kalite Yönetim Sistemi ve ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı uyumlaşma çalışmaları kapsamında Risk Değerlendirme ve Risk İşleme süreci **Risk Yönetimi Prosedürü'** nde tanımlanmıştır. Bu dokümanda Risk yönetimi için, bilgi değeri taşıyan varlıkların tespiti ve bunların değerlendirilmesi, Risk Değerlendirme metodolojisi, Risk İşleme adımları ve bu adımlarda uyulacak kurallar tanımlanmıştır.

5. SOA-Uygulanabilirlik Bildirgesi

Risk işleme seçenekleri standardın EK-A bölümünde verilen A.5'den A.18'e 14 kontrol grubu içerisinde 114 farklı kontrol listesinden seçilebilir. Seçilen kontrollerin her birinin seçilme amacı, kontrolün içeriği, kontrolün uygulanma biçimi ve uygulanmıyorsa nedeni kısa adı **SOA** (**Statement of Applicability**) olan dokümanda belirtilmektedir. *SOA Gizli bilgi sınıfındadır ve yalnızca BGYS Birimi ve BGYS Komisyonunun erişimine açıktır.*

Bilgi güvenliği amaçları ve uygulamaları SOA' da detaylandırılmıştır. Risk Yönetim planı ve SOA paralel dokümanlardır ve beraber incelenmektedir. Risk işleme planında seçilen kontrollerin isimleri veya EK-A'dan seçilmişlerse A.X.X şeklinde kontrol numarasına atıf yapılırken SOA' da kontrol detaylandırılmıştır.
Uygulanan ve uygulanacak tüm kontroller SOA' da kaydedilir. Bu doküman, Risk Yönetim planı ile bir çapraz kontrol sağlayarak herhangi bir kontrolün atlanmamasını sağlamaktadır.

6. Bilgi Hassasiyeti ve Riskler

6.1. Bilgi Varlıklarımız

Masaüstü bilgisayarlar, laptoplar, CD ve DVD ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (internet, e-mail, telefon vb.) yer alan tüm veriler **Şirketimiz** için bilgi varlığı olarak tanımlanmıştır.

6.2. Varlık Sınıflandırması

Şirketimiz içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmıştır. Bu sınıflandırmaya göre;

Halka açık bilgiler, web sitesinde yayınlanan veya 3. Şahıslara verilmesinde, ifşa edilmesinde sakınca bulunmayan her türlü basılı veya dijital olarak saklanan başvuru formu, şartname vb. bilgilerdir.

Şirkete özel bilgiler, şirket içinde sadece çalışanlara açık olan bilgilerdir. Kurum dışından yetkisiz kişilerce erişilmemesi gereken bilgilerdir.

Gizli bilgiler, en kıymetli, bütünlüğü ve gizliliği en kritik olan bilgilerdir. Bu bilgilerin korunması hem iş sürekliliği açısından hem de yasal gereksinimler bakımından son derece önemlidir. Gizli bilgi sınıfındaki tüm varlıklar için kontrol ve koruma metotları tanımlanmış ve yönetilmektedir.

Bilgi Sınıflandırma Kılavuzu

Şirketimiz' de Bilginin **G**izliliği, **B**ütünlüğü ve **E**rişilebilirliğini sağlamaya yönelik, **Şirketimiz** bünyesinde üretilen bilgi aşağıdaki verilen tabloda detayları verilen şekilde sınıflandırılmıştır.

Şirketimiz' in bünyesinde tanımlı süreçlerde oluşan bilgiler önem derecesine göre Halka Açık, Kişisel, İç Kullanım, Şirkete Özel ve Gizili şeklinde sınıflandırılmaktadır. Sınıflandırma ile ilgili gerekli açıklamalar ve saklama yerleri aşağıdaki tabloda açıklanmıştır.

Bilgi Sınıfı	Açıklama	Saklama Yeri
Halka Açık	3. Şahısların bilmesinde sakınca olmayan, genel ya da şirkete özel bilgilerdir. Bu bilgiler müşterilere, iş ortaklarına, tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Dolaplar ve dolap dışlarında, web sitelerinde, her türlü ortam üzerinde.
Şirkete Özel	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın ortak dolapları.
Gizli	En kritik bilgilerdir, sadece yönetim ve yapılan işe özgü ilgili personeller tarafından erişimi vardır. Bu tür bilgilerin yetkisiz erişilememesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır.	Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda/dolaplarda/çekmecelerde veya kişisel bilgisayarlarda tutulur.

Halka Açık Bilgi sınıfı yeşil renk ile yukarıda belirtilmiş, ancak uygulamada bu sınıf için etiket kullanılmamıştır. Dolayısıyla renk etiketi bulunmayan varlıklar "Halka Açık Bilgi" sınıfında kabul edilmektedir.

6.3. Kritik varlıklar

Çalışanlar, sunucular, masaüstü ve dizüstü bilgisayarlar, evrak dolapları, şirkete ait form, plan, çizim, rapor gibi bilgiler ile müşteri verileri kritik varlıklar olarak değerlendirilmektedir. Bu varlıklar risk yönetiminde ve kontrol seçiminde öncelik verilecek olanlardır. Bu varlıkların içerdiği bilgiler Gizli olarak kabul edilmiş ve bilginin Gizliliği, Bütünlüğü ve Yetkilendirilmiş Yöneticilerin Erişilebilirliği ve İş Sürekliliği sağlanmıştır.

7. Bilgi güvenliği politika, prosedür ve rehberleri

BGYS Politikası, şirketimizce yayınlanan birçok politika, prosedür, talimat ve rehberi seçilen kontroller ve risk yönetimi hedefleri çerçevesinde adreslemiştir. Bilgi sistemleri tarafından yayınlanan bu dokümanda genel bilgi güvenliği kuralları tanımlanmıştır. Her çalışan bu dokümanda belirtilen kurallara uyması için gerekli önlemler alınmıştır.

Bilgi yedekleme, bilgi güvenliği ihlal olayı müdahale, iç denetim, doküman ve kayıtların kontrolü, kullanıcı tanımlama, iş sürekliliği planı, acil durum eylem planı, risk işleme planı gibi prosedür ve planlarda sistemin işleyişi anlatılmıştır. İlgili çalışanlar yönetimce tanımlanan ve yayınlanan bu prosedür ve planlara uygun hareket etmektedir.

Hazırlayan	Onaylayan
Yönetim Temsilcisi	**Genel Müdür**

Tüm çalışanlar, şirketimizce tanımlanmış ve yayınlanmış ***gizlilik sözleşmelerini*** imzalayarak kurum politikalarına uyacaklarını taahhüt etmiştir. Taahhütname ve kurallar farklı dokümanlardır. **Personel Gizlilik Sözleşmesi** (Taahhütnamesi) işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.

8. Bilgi Güvenliği Eğitimleri ve Yeterlilik

Şirketimiz' in yapısı, hizmet verdiği süreçler tanımlanmış ve ilgili süreçlerde istihdam ettirilecek personel için hizmet yeterlilik kriterleri personel için görev yetki ve sorumluluklar tanımlanmıştır. Personel istihdamları **İnsan Kaynakları Prosedürü** hükümlerine göre yürütülmektedir.

Tüm **Şirketimiz** çalışanlarına bilgi güvenliği bilinçlendirme eğitimleri düzenlenmiştir. Yönetim çalışanların tamamına bilgi güvenliği yönetim sistemimin gerekliliklerini, amaçlarını, kurallarını ve yaptırımlarını öğretmiş, farkındalık sağlanmıştır. İşe yeni giren tüm çalışanlara uyum eğitimleri kapsamında bilgi güvenliği eğitimleri verilmesi sağlanmıştır.

BGYS Komisyonu üyelerine bilgi güvenliği yönetim sistemi kurulumu ve risk yönetimi eğitimi verilmiştir.

Yönetim, BGYS birimi ve çalışanların bilgi güvenliği konusunda farkındalığın artırılması ve eğitimi için gerekli kaynakları tahsis etmektedir.

9. Doküman ve Kayıtların Kontrolü

BGYS ile ilgili dokümanların hazırlanması, yayınlanmadan önce onaylanması, değişikliklerinin-revizyonlarının takibi, gerekli noktalarda doğu versiyonun ulaşılabilir olması amaçlarını yerine getirecek Dokümante edilmiş **Doküman ve Kayıtların Kontrolü Prosedürü** hazırlanmıştır. Dokümanların kontrolü bu prosedüre uygun olarak yapılmaktadır.

Kayıtların kontrolü, saklanması, yedeklenmesi, gerektiğinde tekrar elde edilebilmesini sağlamak amacıyla da yukarıdaki prosedür hazırlanmış ve uygulanmaktadır.

10. Bilgi Güvenliği İç Denetimleri

Kurulan bilgi güvenliği yönetim sisteminin standarda ve tanımlanan politika ve prosedürlere uygunluğunun tespiti için düzenli olarak gerçekleştirilecek iç tetkikler planlanmıştır. İç tetkiklerin nasıl gerçekleştirileceği **İç Tetkik Prosedürü** tanımlanmıştır ve bu prosedüre uygun olarak düzenli iç tetkikler yapılarak sistemdeki uygunsuzluklar tespit edilmektedir.

11. Sürekli İyileştirme ve Düzeltici Faaliyetler

İç tetkiklerde, ihlal olaylarıyla veya çalışanların kendi gözlemleriyle tespit ettikleri uygunsuzlukların tespitinde ve standarda, politikalarımıza, prosedür ve kurallarımıza uymayan durumların tespitinde ortaya çıkan uygunsuzluğun nasıl giderileceği ve potansiyel uygunsuzlukların nasıl düzeltileceğine ilişkin **Düzeltici Faaliyet Prosedürü** ve **BG İhlal Olayları Yönetimi Prosedürü** hazırlanmış ve uygulanmaktadır. Tüm personel düzeltici faaliyetlere katılmakla sorumludur.

Hazırlayan	Onaylayan
Yönetim Temsilcisi	**Genel Müdür**

Bilgi Güvenliği Politikası Web Versiyon

Şirketimiz üst yönetimi BGYS politikasını; işletmemizin verdiği hizmetlerin sorumluluklarına, mevzuat şartlarına uyma ve etkinliğinin sürekli iyileştirilmesi taahhüdünü içerecek, BGYS hedeflerinin oluşturulması ve gözden geçirilmesi için bir çerçeve oluşturacak şekilde belirlemiştir.

Şirketimiz üst yönetimi BGYS politikasının iletilmesini ve anlaşılmasını sağlar ve sürekli uygunluk için yönetimin gözden geçirmesinde gözden geçirir.

Şirketimiz yönetimi olarak, misyon ve vizyonumuza bağlı olarak, anlaşmalı olduğumuz müşterilerimize Bilgi teknolojileri hizmetinin verilmesi öncelikli çalışma alanımızdır.

Üretim ve Hizmetlerimiz;

- Müşterilerimizin, sözleşme dahilinde hizmet verdiğimiz kurum / kuruluşların beklentilerini yüksek düzeyde karşılamak, bilgi işlem yeteneklerini artırmak, teknolojik gelişmelerden haberdar ederek faaliyet / proses / performans hedeflerine ulaşmalarına yardımcı olunması BGYS kapsam ve sınırları içinde sürdürülmektedir.
- BGYS kapsamı ve sınırları içinde hizmet verdiğimiz tüm bilgi teknolojileri sistemlerinde işlenen her türlü gizli / ticari / özel bilginin, hizmet verdiğimiz kurum / kuruluşun müşterisinin mahremiyeti olduğunu kabul ederek, bu bilginin herhangi bir yerde / kişi / kurum / kuruluşta müşterinin bilgisi / onayı olmaksızın Gizlilik / Bütünlük / Elverişlilik şartlarına bağlı kalarak elde edilemezliği sağlanmıştır.
- **Şirketimiz** BGYS kapsam ve sınırları içinde kalmak koşulu ile BGYS politikası, yasal ve düzenleyici gereksinimlere uyacak, sözleşmelerden doğan veya üçüncü şahısların yükümlülüklerini veya bağımlılıkları dikkate almaktadır.

Şirketimiz, yukarıda ifadesi bulan çerçeve içinde Bilgi Güvenliği Yönetim Sisteminin (BGYS) kurulumuna, gerçekleştirilmesine, işletimine, izlenmesine, gözden geçirilmesine, bakımına ve iyileştirilmesine olan bağlılığını aşağıdaki hususları gerçekleştirerek kanıtlayacağını beyan eder:

- BGYS amaçları tanımlanmış ve planları yapılmıştır.
- Risk analizlerini yapılmış, analiz sonuçlarına bağlı olarak risk değerlendirmelerini ve risk kriterlerini ortaya koymuş, bu çerçevede risk yönetimini sağlamaktadır.
- Bilgi güvenliği amaçlarını karşılamanın ve bilgi güvenliği politikalarına uyumun önemini, yasaya karşı sorumluluklarını ve sürekli iyileştirmeye olan gereksinimi tanımlamış ve sürekliliğini sağlamıştır.
- BGYS' yi kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek

için yeterli kaynakları (finansal, insan kaynakları, ekipman, yazılım, güvenlik, danışmanlık, eğitim vs.) sağlamıştır.

- Riskleri kabul etme ölçütlerini ve kabul edilebilir risk seviyelerini belirlemek üzere gerekli çalışmaları organize etmiş ve yönetmektedir.
- Yılda en az bir kez BGYS Politikasını gözden geçirerek ve gerekli gördüğü hallerde düzenlemeleri yaparak ilgili taraflara duyuracaktır.