BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	**:** 2019/BİM/KI_BGP
Doküman Adı	**:** Bilgi Güvenliği Politikası
Yayın Tarihi	**:** 15.09.2019
Revizyon No	**:**
Revizyon Tarihi	**:**
Süreç Sorumlusu	**:** Bilgi İşlem Merkezi ve İç Denetim Müdürlüğü
Hazırlayan	**:** Bilgi İşlem Merkezi
Kullanan	**:** Denge Varlık Yönetim A.Ş.

Doküman Revizyon Tarihçesi

Revizyon Tarihi	Yazan	Revizyon No	Revizyon Açıklaması
15/02/2023	Onur Eren	1	Güncelleme Yapılmamıştır.

İÇERİK

1. AMAÇ

Bu politikanın amacı, bilgiyi yaşam döngüsünün her safhasında ve her bilgi saklama ortamında, yetkisiz erişimden, kasıtlı veya kasıtsız hatalı kullanım ve değişiklikten, bozulmaktan ve yok edilmekten korumaktır. Bu şekilde bilginin kullanılabilirliğinin, gizliliğinin ve bütünlüğünün sağlanması hedeflenmektedir.

2. KAPSAM

Bu politika, bilgi saklama ortamlarında var olan, Şirket'e ve müşterilere ait tüm bilgileri kapsamaktadır. Bu politikada bilgi saklama ortamlarında, Şirket'in sahip olduğu tüm Bilgi İşlem uygulamaları ve sistemleri ile bunlarla ortak çalışan her tür bilgi saklama, yedekleme, arşivleme birimleri ve ekipmanları tanımlanmıştır.

Bilginin güvenliği ve güncellenmesine ilişkin hususlar, kimlerin bilgiye erişeceği vb. konular ile ilgili kararlar, Bilgi İşlem Merkezi'nin önerisi ve bilginin sahibi olan birimlerin onayı ile yürürlüğe konulur.

3. BİLGİ GÜVENLİĞİ POLİTİKASI

3.1. Bilgi Güvenliği Organizasyonu

Şirket yönetimi, bir bilgi güvenlik sorumlusu atayıp, bilgi güvenliği meselelerini koordine edecek ve yönetecek rol ve sorumlulukları dağıtır.

Şirket'in faaliyetleri sonucu üretilen tüm bilgiler, Şirket'in mülkiyetindedir. Çalışanların bireysel olarak yürüttükleri çalışmalar sonucu üretilen bilgi de bu kapsam içinde yer alır.

Tüm personelin Bilgi Güvenliği Politikası'nı okuması sağlanır. Ayrıca tüm çalışanlar Bilgi Güvenliği Politikası'nı okuduğu ve kabul ettiğine dair taahhütname imzalar ve bu taahhütnameler personel dosyalarında saklanır.

Müşteri bilgileri ile Şirket'e ait özel bilgiler sadece; müşterinin yazılı izni olduğu, yasal olarak yetkili birimlerin talebi ya da kanuni zorunlulukların gerektirdiği durumlarda üçüncü şahıslara açıklanabilir.

3.2. Rol ve Sorumluluklar

3.2.1. Yönetim Kurulu

Yönetim Kurulu, Bilgi Güvenliği Politikasının onaylanması, Şirket'in tüm personeline dağıtımının sağlanması ve bilgi güvenliği raporlarını değerlendirmekten sorumludur.

Yönetim Kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı gösterir, bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder ve aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

- Bilgi güvenliği politikalarının ve tüm sorumlulukların belirli periyotlarla gözden geçirilmesi ve onay mekanizmasına tabi tutulması
- Bilgi kaynaklarına yönelik risklerin ve bilgi güvenliği ihlaline ilişkin olayların periyodik olarak değerlendirilmesi

3.2.2. İç Denetim Müdürlüğü

İç Denetim Müdürlüğü; Şirket çapında bilgi güvenliği yönetim çevresinin uygulanmasının takibinden; bilgi güvenliği bilincinin oluşturulmasından; bilgi güvenliği stratejilerine yön vermekten; bilgi güvenliğine yönelik politika, prosedür, standart ve talimatları önermekten ve gözden geçirmekten; bilgi güvenliğini tehdit eden riskleri tanımlamaktan; kendisine düzenli sunulan bilgi güvenliği raporlarını değerlendirmekten; bilgi güvenliğine yönelik tüm yasal yükümlülüklerin teknik detaylarının hayata geçirilmesi için yönlendirmekten; güvenlik denetimleri sonucu ortaya çıkan bulgu ve açıklıkların takibini koordine etmekten; Bilgi Güvenliği Politikası'ndaki güncellemeleri Yönetim Kurulu'na sunulacak şekilde onaylamaktan sorumludur.

3.2.3. Bilgi İşlem Merkezi

Politika çerçevesinde ele alınan konuların ve stratejilerin hayata geçirilmesi ve uygulamasından; iş yapış şekillerini Yönetim Kurulu ve İç Denetim Müdürlüğü'nün aldığı kararlar ve stratejiler doğrultusunda Şirket'te oluşturulan politika, prosedür ve standartlara adapte etmekten ve uygulamaktan; Bilgi Güvenliği Politikası'nın ve eklerinin uygulanıp uygulanmadığını belirli aralıklarla kontrol etmekten; güvenlik olayları ile ilgili araştırma yapmaktan; hazırlanan güvenlik farkındalık eğitimlerinin içeriğini ve şeklini oluşturmaktan ve Şirket içindeki güvenlik kontrollerinin durumunu İç Denetim Müdürlüğü'ne düzenli olarak raporlamaktan sorumludur.

3.2.4. Personel/Kullanıcı

Tüm Şirket personeli, gerek bu politikada gerekse destekleyici diğer prosedürler ile standartlarda belirtilen bilgi güvenliğine yönelik Şirket yaklaşımına uygun bir şekilde hareket etmekten ve çalışmalarında bunları uygulamaktan sorumludur.

3.3. Prosedürler ve Standartlar

3.3.1. Bilgi Varlıklarının Sınıflandırılması

Şirket, işlenen veya saklanan verinin ve bu veriyle ilgili tüm varlıkların gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayarak kazara veya kasti biçimde hasar görmesi, değişmesi, ifşa olması veya kaybolmasını önler. Bunun için varlık değerlendirmelerini yaparak bilgilerini sınıflandırır. Bilgi varlıkları, mümkün olduğu durumlarda, bilgi sınıflandırmasını yansıtacak şekilde etiketlenir. Her varlığa bir sahip atanır.

3.3.2. Bilgi İşlem Risk Yönetimi

Varlıklarla ilgili oluşabilecek riskler değerlendirilir ve bu riskler izlenir. Kontrol uygulayarak azaltılabilecek veya transfer edilebilecek risklerle ilgili kontroller oluşturulur, geri kalan riskler de Üst Yönetim tarafından değerlendirilerek kabul edilir. Şirket'te bilgi güvenliği kontrollerinin etkin bir şekilde hayata geçirilmesi için bilgi teknolojileri varlıklarının risk değerlendirmelerinin ve maruz kaldıkları riskler için kontrol oluşturma çalışmalarının yapılması ve Bilgi İşlem risklerinin kontrol altına alınması için ilgili tüm personel tarafından Bilgi İşlem Risk Yönetimi Prosedürü'ne uyumlu davranılır. .

3.3.3. Şifre Yönetimi

Bilgi sistemleri ortamlarına erişirken kullanılan şifrelerin standartlara uygun biçimde oluşturulması, korunması, kullanılması ve değiştirilmesi, kullanıcılara tanımlanan şifreler konusunda çalışanların bilgilendirilmesi ve şifre işlemlerinin riski en aza indirecek en güvenli şekilde yapılmasını sağlamak amacıyla gerekli süreçler oluşturulur ve uygulanır. Bu süreç çerçevesinde, şifre oluştururken ve kullanırken uygulanacak genel kurallar, ana uygulama ve diğer sistemler için şifre parametrelerinin tanımlandığı Bilgi İşlem Erişim Standartları'na tüm personel tarafından uyumlu davranılır.

3.3.4. Fiziksel ve Çevresel Koşullar

Şirket faaliyetlerinin gerçekleştirildiği yerlerde, işlenmekte olan bilginin değerine uygun şekilde fiziksel güvenlik önlemleri Şirket tarafından alınır. Başta kritik yazılımlar ve donanımlar olmak üzere Şirket bilgi sistemlerinin fiziksel ve çevresel güvenliğinin korunması/arttırılması amacıyla oluşturulan Fiziksel ve Çevresel Güvenlik Standartları'na tüm personel tarafından uyumlu davranılır.

3.3.5. Sistemlere Erişim ve Yetkilendirme

Şirket'in bilgi sistemlerine erişimde kullanılan kullanıcı hesaplarının yaratılması, izlenmesi ve silinmesi standartlarını tanımlamak, kullanıcıların erişmeye yetkili olacağı uygulamaları ve sistemleri belirleyerek, diğer sistem ve uygulamaları yetkisiz erişimlere karşı korumak amacıyla oluşturulan Bilgi İşlem Yetkilendirme Prosedürü ile Bilgi İşlem Erişim Standartları'na tüm personel tarafından uyumlu davranılır.

3.3.6. Internet Kullanımı ve E-posta Güvenliği

İnternet'in uygun olmayan kullanımı, Şirket'in yasal yükümlülükleri, kapasite kullanımı ve profesyonel imajı açısından istenmeyen sonuçlara neden olur. Bilerek ya da bilmeden, bu türden olumsuzluklara neden olunmaması amacıyla İnternet'in kurallara, etik ve yasalara uygun kullanımı sağlanır. Kabul edilebilir ve edilmez İnternet kullanımı ile yasaklı web alanlarının tanımı ve açıklaması yapılır.

E-posta, en önemli iletişim kanallarından biridir. E-postalar gönderilirken bilgi gizliliğine dikkat edilir. Üst Yönetim tarafından e-posta gönderimine ilişkin alınan karalar tüm personele iletilerek uyum konusunda gerekli özenin gösterilmesi sağlanır. Ek olarak, e-posta güvenliğine ilişkin gerekli teknolojik kontrollerin oluşturulması Yönetim Kurulu sorumluluğundadır.

3.3.7. Veri Güvenliği

Bilginin, Bilgi İşlem sistemlerine yetkilendirilen kişilerce kontrollü biçimde kaydedilmesi, gizlilik, bütünlük ve kullanılabilirlik ilkeleri doğrultusunda Bilgi İşlem sistemlerinde tutulması ve kullanılması, belirlenen ortamlarda belirlenen süre boyunca yedeklenmesi ve arşivlenmesi, süre bitiminde de imha edilmesi sağlanır. Kamuya açık bilgilerin dışında kalan her türlü bilgiye ve veri işleme kaynaklarına sadece kimliği tanımlanmış, kimliği doğrulanmış ve yetkilendirilmiş kişiler, yetkileri dâhilinde erişir. Bu süreçlerin tanımlandığı Bilgi İşlem Veri Yönetimi Standartları ile Veri Sınıflandırma Çalışması dokümanlarına ilgili tüm personel tarafından uyumlu davranılır.

3.3.8. Zararlı Yazılımlardan Korunma

Hiçbir istisna olmadan, tüm kullanıcı PC'leri, sunucular ve taşınabilir bilgisayarlara anti-virüs yazılımı kurulur; düzenli güncellemelerinin ve taramaların yapılması sistem tarafından sağlanır.

Anti-virüs yazılımı, konusunda uzman ve lider olan bir sağlayıcıdan alınır.

Dışarıdan gelen e-postalar oluşturdukları bilgi güvenliği riskleri göze önünde tutularak özenle ele alınır. Kurum e-posta sunucusuna gelen mesajlar ile ekleri yalnızca virüs taramasından geçtikten ve onaylandıktan sonra iç ağa indirilir.

Yanıltıcı virüs uyarılarına karşı kurum çalışanları bilgilendirilir ve gerekli önlemler alınır.

3.3.9. Lisanslı Yazılım Kurulum ve Kullanımı

Şirket, bünyesinde yer alan bilgisayarlarda lisanssız yazılımların kurulumunu ve kullanımını engeller. Bilgi İşlem Merkezi izinsiz kurulan ve kontrolsüz kullanılan yazılımları tespit eder ve bilgi sistemleri üzerinden siler.

3.3.10. Güvenlik Olaylarının Bildirimi

Şirket bünyesinde, güvenlik olaylarının bildirimi bizzat personelin kendisi tarafından mümkün olan en kısa sürede direk Bilgi İşlem Merkezi'ne telefon ya da e-posta aracılığıyla yapılır. Şirket'in bilgisayar ağında oluşabilecek güvenlik ihlalleri karşısında nasıl davranılacağının belirlenmesi, güvenlik olaylarının sebeplerini analiz edebilmek için gerekli ve yeterli sayıda verinin toplanması ve güvenlik olaylarından sonra sistemin en kısa sürede tekrar çalışır duruma getirilmesi Bilgi İşlem Merkezi'nin sorumluluğundadır. Tüm çalışanlar, şahit oldukları güvenlik ihlallerini sorumlu birimlere iletmekle yükümlüdür.

3.3.11. Şirket Dışına Veri Transferi

Şirket dışına gönderilen tüm veriler için verilerin gizliliği, bütünlüğü ve veri transferine konu olan tarafların kimliklerinin doğrulanması için yeterli kontroller oluşturulur. Transfer edilecek veri için alınacak güvenlik önlemlerine ilişkin kontroller, verinin Veri Sınıflandırması dokümanında belirlenen sınıfına göre Bilgi İşlem Merkezi tarafından belirlenir. Fiziksel olarak yapılan veri transferlerinde sadece yetkili ve güvenli kuryeler kullanılır. Yetkisiz erişimleri engellemek amacıyla parçalara bölerek ya da şifreleyerek gönderme yapılır.

3.3.12. Denetim İzlerinin Yönetilmesi

Şirket'in tüm kritik sistem ve uygulamalarının denetim izleri Bilgi İşlem Merkezi sorumluluğunda saklanır, takip ve analiz edilir. Böylece gerekli görüldüğünde kullanıcı faaliyetleri hakkında detaylı bilgi toplanabilir. Denetim izlerin yönetilmesi için oluşturulan Bilgi İşlem Denetim İzi Yönetimi Standartları'na ilgili tüm personel tarafından uyumlu davranılır.

3.3.13. Bilgi Sistemleri Yazılımlarının Alınması, Geliştirilmesi ve Bakımı

Yeni bir yazılım temin edilirken veya mevcut yazılımlarda değişiklik yapılırken; ilgili güvenlik ihtiyaçları, analiz safhasında ele alınır ve güvenlik ihtiyaçları göz önünde bulundurulur. Şirket, yazılımlar için değişiklik kontrol süreci uygular ve sistemleri buna uygun şekilde günceller.

Şirket politikası gereği dışarıdan tedarik edilen hizmetlere ilişkin tedarikçi çalışanları Şirket Bilgi Güvenliği Politikası'na ek olarak Bilgi İşlem Tedarikçi Yönetimi Prosedürü ile Bilgi İşlem Değişiklik ve Problem Yönetimi Prosedürü'ne uymakla zorunludur.

3.3.14. İş Sürekliliği Yönetimi

Faaliyetlerin devamını sağlamak ve kritik iş faaliyetlerini çeşitli arızalardan ve felaketlerden koruyarak kısa sürede yeniden başlatabilmek için iş sürekliliği ana çatısı oluşturulur ve uygulanır. Bu plan, düzenli olarak test edilir ve değişikliklere karşı gözden geçirilir. Kritik faaliyetlerde kullanılan verilerin yedeği alınır. Şirket'in karşılaşması muhtemel olağandışı olaylar ve felaketler karşısında hazırlıklı olması ve iş sürekliliğini sağlamak amacıyla hazırlanan Felaket Kurtarma Standartları'na tüm personel tarafından uyumlu davranılır.

3.4. Güvenlik Farkındalık Eğitimleri

İnsan Kaynakları ve Eğitim Birimi, Şirket personelinin bilgi güvenliğine yönelik farkındalıklarını arttırabilmek amacıyla, çeşitli dönemlerde eğitimler düzenler. Bu eğitimlerin içeriği ve formatı, Bilgi İşlem Merkezi tarafından oluşturulur ve güncellenir.

Bu eğitimler çerçevesinde Şirket Bilgi Güvenliği Politikası ve ilgili prosedürler ile standartlar personele aktarılır ve personel tarafından rol tanımlarının bilinmesi/sahiplenilmesi sağlanır.

3.5. Personeli İlgilendiren Konular

Şirket'in tüm personeli Bilgi Güvenliği Politikası'nı okuyup kabul ettiğine dair taahhütname imzalar ve bu taahhütnameler İnsan Kaynakları ve Eğitim Birimi tarafından saklanır. Bilgi Güvenliği Politikası güncellemeleri Bilgi Güvenliği Sorumlusu tarafından tüm personele e-posta ile duyurulur.

Aşağıdaki durumlardan en az birinin gerçekleşmesi durumunda Bilgi Güvenliği Politikası'nın ihlal edildiği sonucuna varılır:

- Şirket bilgilerini ve bilgi güvenlik sistemini tehlikeye atarak Şirket'i fiili ve olası iş kaybına maruz bırakmak,
- Şirket'in itibarını riske atmak,
- Şirket bilgilerini yetkisiz bir şekilde kullanmak, ifşa etmek, değiştirmek, tahrip etmek ve/veya bu bilgileri izinsiz bir şekilde üçüncü kişilerle yazılı/elektronik olarak herhangi ortamda paylaşmak

Şirket, Bilgi Güvenliği Politikası'nın ihlali durumunda bu ihlalin ciddiyetine göre hareket etme hakkını saklı tutar; ancak Politika'ya uymama veya kasıtlı Politika ihlalleri, disiplin cezası, yazılı kınama, işten çıkarma, hukuk muameleleri ve/veya cezai kovuşturmalar dahil olmak üzere bunlarla sınırlı olmayan eylemlerle sonuçlanabilir. Şirket, ihlalin ciddiyetine göre, çalışanın sistemlere erişim haklarını ve ilgili sorumluluklarını askıya alabilir.

3.6. Yasal Yükümlülükler

Şirket'in tabi olduğu sektörel kanun, yönetmelik ve düzenlemelerde belirtilen şartların yerine getirilmesinden Yönetim Kurulu ve İç Denetim Müdürlüğü sorumludur. Bilgi güvenliğine yönelik tüm yasal yükümlülüklerin teknik detaylarının hayata geçirilmesinden ise Bilgi İşlem Merkezi sorumludur.

3.7. Güvenlik Denetimi ve Uyum

Tüm çalışanlar ilgili yasalara, yönetmeliklere, fikri mülkiyet haklarına, lisans anlaşmalarına, Şirket politika ve prosedürlerine uymakla yükümlüdürler. Tüm çalışanlar, kurum verilerinin saklanması ve gizlilik derecelerine uygun şekilde ele alınması konusunda sorumludurlar.

Şirket, gerek bağlı bulunduğu sektörel düzenlemeler sebebiyle gerekse bilgi güvenliğine yönelik kontrollerin arttırılması amacıyla İç Denetim Müdürlüğü aracılığıyla denetim faaliyetleri gerçekleştirir.

3.8. Politikanın Gözden Geçirilmesi ve Güncellenmesi

Bilgi Güvenliği Politikası, gerektiğinde veya en az yılda 1 (bir) kere gözden geçirilir ve gerekli ise Yönetim Kurulu onayı ile yeniden yayınlanır. İş birimleri; Bilgi Güvenliği Politikası ve bu politikada belirtilen standartların uygulanması konusunda, değişiklik, ek ya da çıkartma taleplerini detaylı gerekçeleri ile Bilgi İşlem Merkezi'ne bildirebilirler. Ek olarak, sorumlu birimler tarafından gerek duyulduğunda gözden geçirme dönemi beklenmeden de politikada değişiklik önerileri hazırlanarak Yönetim Kurulu onayına sunulabilir.

Bilgi Güvenliği Politikası gözden geçirilirken aşağıda listelenen hususlar özellikle göz önünde bulundurulur:

- Mevcut politikanın etkinliği ve yeterliliği
- Tercih edilen güvenlik önlemlerinin ve korunan varlıkların değerleri
- Teknolojideki değişiklikler

4. EKLER

- Bilgi İşlem Değişiklik ve Problem Yönetimi Prosedürü
- Bilgi İşlem Yetkilendirme Prosedürü
- Bilgi İşlem Tedarikçi Yönetimi Prosedürü
- Bilgi İşlem Risk Yönetimi Prosedürü
- Bilgi İşlem Denetim İzi Yönetimi Standartları
- Bilgi İşlem Erişim Standartları
- Bilgi İşlem Fiziksel ve Çevresel Güvenlik Standartları
- Bilgi İşlem Veri Yönetimi Standartları
- Bilgi İşlem Felaket Kurtarma Standartları
- Veri Sınıflandırması Çalışması