1-Amaç

Bilgi Güvenliği Politikası' nın amacı, şirket genelinde uygulanacak temel bilgi güvenliği prensiplerini belirlemek ve Şirket Yönetim Kurulu'nun konu prensiplere verdiği destek ve önemi ifade etmektir.

2-Kapsam

Şirket stratejik hedeflerinin desteklenmesi, sahip olunan marka değerinin korunması ve ilgili düzenlemelere uyumun sağlanması amacıyla izlenmesi gereken bilgi güvenliği kuralları Bilgi Güvenliği Politikası kapsamında yer almaktadır.

Bilgi Güvenliği Politikası'nın hedef kitlesi, şirket çalışanları, şirket mülkiyetinde ya da kullanımında olan bilişim sistemi ya da bilgi varlığına erişim yetkisi verilen iş ortakları, tedarikçi/ler ve diğer kullanıcılardır.

3-Roller ve Sorumluluklar

Rol	Sorumluluk
Yönetim Kurulu	Bilgi güvenliği gereksinimlerinin tespit edilmesi amacıyla Bilgi Güvenliği Politikası'na onay verir ve söz konusu politika çerçevesinde gerçekleştirilmesi gereken faaliyetlerin takip edilmesi amacıyla "Bilgi Teknolojileri Sorumlusu'nu" görevlendirir.
Personel	Şirket mülkiyetinde ve kullanımında olan bilgi ve bilişim sistemi varlıklarının güncel tehditlere karşı korunması için sorumluluk alanlarına düşen görevleri gerçekleştirmek ve konu ile ilgili kurallara uygun hareket etmekle yükümlüdür.
Bilgi Teknolojileri Sorumlusu	Şirket genelinde uygun güvenlik ve bilgi güvenliğine yönelik kontrollerinin belirlenmesi/uygulanması/ koordine edilmesi konularından sorumludur.
Tedarikçi	Şirket iş süreçlerinin işletilmesi amacı ile ihtiyaç duyulan kaynak ya da hizmetlerin sunulmasında gerekli bilgi güvenliği gereksinimlerine uymakla yükümlüdür.
İş Ortağı	Ortağı olduğu/oldukları Şirket iş süreçlerine ait bilgi güvenliği gereksinimlerinin sağlanması amacıyla ilgili sözleşmeler ve/ve ya anlaşmalar çerçevesinde hareket etmekle yükümlüdür.

4- Bilgi Güvenliği Politikasına İlişkin Temel İlkeler

Bilgi Güvenliği Politikası; ilgili düzenlemeler ile Şirket için belirlenen görev ve sorumlulukların kesintisiz sürdürülmesi, vizyon ve misyon hedeflerine ulaşılması, kurum stratejik planlarının gerçekleştirilmesi, kurumun, müşterilerin, çalışanların ve iş ortaklarının bilgilerinin korunması amacıyla kurum bünyesinde işletilen iş süreçlerine ait bilgi güvenliği kuralları/prensipleri çerçevesinde yürütülmesini sağlar.

Şirket bünyesinde işletilen tüm iş süreçlerinin tasarımı ve işletimi aşağıda belirtildiği şekilde "bilgi güvenliği" kuralları/ prensipleri çerçevesinde gerçekleştirilir.

4.1 Şirket iş süreçlerinin tasarım ve işletilmesi konularında söz konusu süreçlerin bilgi güvenliği gereksinimlerinin belirlenmesi ve bu belirlenen gereksinimlerin karşılanması amacı ile etkin yöntemlerin uygulanması esastır. Şirket bilgi güvenliğinin uluslararası standartlar doğrultusunda yönetilmesi ve sağlanması ile ilgili bilgi güvenliği prensiplerine uyum esastır.

4.2 Şirket iş süreçleri tasarımında, aynı zamanda işletiminde bilinen bilgi güvenliği riskleri değerlendirilme altına alınarak kalan ve kabul edilenler dışındaki risk olasılıklarını ve etkilerini azaltıcı bilgi güvenliği kontrolleri (Belgenin devamında "kontrol" ibaresi ile ifade edilecektir) oluşturulur. Risk değerlendirme faaliyetinin ve kontrollerin etkin biçimde işletilmesi iş süreci sahibinin sorumluluğundadır.

4.3 Şirket mülkiyetinde olan her türlü bilgiyi yada bilişim sistemini hedef alan olası bilgi güvenliği tehditlerine karşı gerek tespit,kayıt altına alma, engelleme, vb. yöntemleri, mekanizmaları hayata geçirilir. Bahsi geçen yöntem ve mekanizmaların güncel tehditlere karşı etkin koruma sağlamasını teminen gerekli güncelleme faaliyetleri yürütülür.

Onaylayan:

4.4 Bilgi varlıklarının taşıdığı bilgi güvenliği risklerinin tamamiyle yok edilmesinin mümkün olmadığı hallerde ve durumda "kalan risk" olacağı bilinci ile mevcut risklerin yönetilmesi, söz konusu kalan riski en az düzeye düşürecek önleyici ve düzeltici tedbirlerin etkin şekilde uygulanması esastır.

4.5 Şirket bünyesinde üretilen, muhafaza edilen, işlenen yada iletilen her türlü bilgi Şirket mülkiyetinde yer almaktadır.

4.6 Bilgi güvenliği kapsamında gerçekleştirilen faaliyetlerin hedeflenen başarıya ulaşabilmesi için kullanıcıların bilinçli yaklaşımı ve sorumluluk alanlarına düşen tüm görevleri yerine getirmesi esastır.

4.7 Bilgi güvenliği konusunda bilinçli olarak hareket etmek, şüphe içeren durumlar ile ilgili bildirimde bulunmak, bilginin güvenliğine ilişkin alınacak önlemlerin uygulanmasına destek olmak, iş sürekliliği faaliyetlerine destek vermek kullanıcıların görev tanımlarının ayrılmaz parçasıdır.

4.8 Kullanıcılar, bilişim sistemleri üzerinde kendilerine tahsis edilen kullanıcı hesap bilgilerinin gizliliğinin korunması amacıyla gerekli tedbirleri almakla yükümlü olup, kendilerine tahsis edilen kullanıcı hesapları ile yapılan işlemlerden de sorumludur.

4.9 Kullanıcılar, kendilerine tahsis edilen tüm hesapların şifrelerini kendilerine bildirilen şifre kombinasyon ve kriterlerine uygun şekilde belirlemekle sorumludur.

4.10 Kullanıcılar yetkileri kapsamında eriştikleri bilginin kaybolmasını, bozulmasını ve yetkisiz erişilmesini önlemek amacıyla koruyucu, düzeltici tedbirleri almakla ve bilginin emanetçisi olması durumunda konuya yönelik tedbirleri uygulamakla yükümlüdür.

4.11 Kullanıcıların yetkilendirilmesinde gerekli olan minimum yetkinin verilmesi ve yetkilerin düzenli olarak kontrol edilmesi sağlanır.

4.12 Dış ağlardan gelmesi muhtemel tehditlere karşı ağ güvenliği tesis edilir.

4.13 Kullanılan şifreleme anahtarlarının güvenilir durumda olması sağlanır.

4.14 Kullanıcı bilgisayarlarına Bilgi Teknolojileri Sorumlusu tarafından belirlenen ve kullanıcı bilgisayarlarına yüklenmiş olan yazılımlar dışında yazılım yüklenemez.

4.15 Taşınabilir aygıtlar yalnızca iş amaçlı olarak kullanılır. Söz konusu cihazların kullanımı, yetkilendirilmiş şahıslar tarafından gerçekleştirilse bile; iş ile ilgili olmayan verilerin dağıtımında kullanılamaz.Yetkilendirilmemiş kullanıcılar bilgisayarlarda taşınabilir bellek kullanamaz/kullanması engellenir.

4.16 Şirket interneti iş süreçlerinin güvenli ve sorunsuz ilerlemesini amaçlar. İş dışı erişimler güvenlik nedeniyle kısıtlanabilir.

4.17 Misafir kullanıcılarının lokal ağa erişimine izin verilmez. Gerekli durumlarda yalnızca fiziksel olarak bağımsız internet ağından güvenli internet erişimleri sağlanır.

4.18 Uzak erişim ihtiyacı duyan kullanıcılara, yönetim onayı sonrasında BT kriterlerine uygun erişim izni verilebilir,bu sayı minimal düzeyde tutulmaya çalışılır.

4.19 Kurumsal anti-virüs yazılımı, tüm son kullanıcı bilgisayar sistemlerine yüklenir ve casus yazılımlara, Truva atlarına, virüslere, solucanlara, reklam yazılımlarına veya rootkit'lere karşı koruma sağlanır.

4.20 Mevzuata ve iş ihtiyaçlarına uygun olarak yedekleme süreçleri işletilir.

4.21 Kurum verilerinin, kurum içerisinde ve/veya dışında, elektronik yada basılı halde taşınması, verinin gizlilik derecesine göre, taşındığı ortama ve taşıyan kişinin yetkisine/yetkilerine bağlı olarak sınırlandırılmış olup, çalışanlar verilerin taşınmasına yönelik olarak belirlenmiş olan güvenlik kurallarına uymalıdır.

4.22 Şirket mülkiyetinde olan bilgi veya bilişim sisteminin bulunduğu fiziksel mekânlara erişim durumu kullanıcıların rolleri ve sorumluluklarıyla uyumlu olacak şekilde sınırlandırılır.

4.23 Şirket mülkiyetinde olan bilgi ve bilişim sistemini hedef alan tüm bilgi güvenliği olayları bilgi güvenliği olay yönetimi kapsamında değerlendirilir. Yapılan değerlendirmeler sonucunda, mevcut kontrollerin güncellenmesi ya da yeni kontrollerin devreye alınması faaliyetleri en kısa sürede gerçekleştirilir.

Onaylayan:

4.24 Tüm personelin erişimini sağlamak amacı ile politika dokümanı ve ilgili diğer dokümanlar Şirket Intranet portalı/şirket dosya dizini üzerinden ulaşılabilir duruma getirilir ya da periyodik zamanlarda personele gönderilir.

4.25 Kişisel bilginin mahremiyetinin korunmasını sağlamak amacıyla müşteri ve personel bilgilerinin gizliliği sağlanır.

4.26 Bilginin bütünlüğünü koruyacak ve sürekli erişilebilir durumda olduğunu garanti altına alacak alt yapı ve kontroller hayata geçirilir.

4.27 Bilginin alındığı, muhafaza edildiği, işlendiği ve iletildiği alanlarda bilginin güvenliğinin sağlanabilmesi için gerekli fiziksel/çevresel güvenlik tedbirleri alınır.

4.28 Belirlenen bilgi güvenliği politikalarına, süreçlerine, yasal ve düzenleyici zorunluluklara çalışanların uymalarına dair yazılı taahhüt alınır.

4.29 Bilgi Güvenliği Politikası tebliğ tarihi; şirket çalışanlarına duyurulduğu tarih olarak sayılır.

5- Bilgi Teknolojisi Sorumlusunun Bilgi Güvenliği Hususlarına İlişkin Sorumlulukları

5.1 Bilgi Güvenliği Yönetim Süreci'nin kurulumuna yönelik yapılan çalışmaları organize etmek ve yapılan çalışmalar ile ilgili yönetimi bilgilendirmek.

5.2 Bilgi Güvenliği ile ilgili projelerin hayata geçirilmesi çalışmalarını koordine etmek.

5.3 Gerekli politika, prosedür ve dökümanların oluşturulması çalışmalarını koordine etmek.

5.4 Yeni başlatılan ve/ve ya devam eden projelerde bilgi güvenliğine yönelik gereksinimleri tespit etmek.

5.5 Açıklık analizi çalışmalarını koordine etmek.

5.6 Bilgi Güvenliği Yönetim Süreci politikalarının ve prosedürlerinin güncel durumda olmasını sağlamak.

5.7 Bilgi güvenliğinin izlenmesi ile ilgili faaliyetleri koordine etmek.

5.8 Bilgi Güvenliği Yönetim Süreci'ne yönelik farkındalığın artırılması amacı ile eğitim/bilgilendirme faaliyetlerinin gerçekleştirilmesini sağlamak.

5.9 Bilgi güvenliğini etkileyen, iç ve dış mevzuat ile ilgili uyum çalışmalarını koordine etmek.

5.10 Meydana gelen atakların takip edilmesini,gerekli tedbirlerin alınmasını ilaveten raporlanmasını koordine etmek.

5.11 Bilgi güvenliğine yönelik eğitim ihtiyaçlarını belirlemek.

5.12 Bütçe hazırlama döneminde güvenlik ile ilgili bütçenin hesaplanmasına destek olmak.

5.13 Bilgi varlıklarına ait riskler ile ilgili konularda gerektiğinde üst yönetime ve yönetim kuruluna danışmanlık yapmak.

5.14 Bilgi Güvenliği Politikasını yılda en az 1 (bir) kez gözden geçirmek ve/ve ya güncellenmesi durumunda üst yönetimin onayına sunmak.

6- Bilgi Güvenliği Politikasının Gözden Geçirilmesi

Şirket Bilgi Güvenliği Politikası Bilgi Teknolojileri Sorumlusu tarafından yılda en az 1 (Bir) kez gözden geçirilir ve gerek duyulması halinde güncellenerek üst yönetim onayına sunulur. Güvenlik teknolojilerindeki gelişmelere bağlı olarak ortaya çıkan ihtiyaçları kapsayacak yeni politikalar üretilir.

Onaylayan:

7-Yürürlük

Bilgi güvenliğine ilişkin bu düzenleme, üst yönetimin onay tarihi itibari ile yürürlüğe girer. Şirket'in bilgi güvenliği ile ilgili tüm uygulama ve iş akışları politika hükümleriyle uyumlu şekilde oluşturulur ve güncellenir.

8- Denetleme ve Politikalara Uyulmaması Durumu

BT sorumlusu ve her birim yöneticisi Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetlemekten ,her personel Bilgi Güvenliği Politikasına uymaktan birinci derece sorumludur.

Bilgi Güvenliği Politikası ihlalleri, şirketin risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca yeni Türk Ceza Kanuna göre de cezai sorumluluk doğurmasına ve maddi zararların tazmini sorumluluğuna sebep olabilecektir. Dolayısıyla söz konusu ihlal aynı zamanda Atasan Personel Yönetmeliği ihlali olup disiplin cezası sonucunu doğuracaktır. Gerek gözetim, gerek denetim, gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlaline neden olan kullanıcılar disiplin kuruluna sevk edilir.

Onaylayan: