Doküman Bilgileri	
Adı:	Bilgi Güvenliği Politikası
Doküman No:	PK-BPL01
Revizyon No:	02
Doküman Tarihi:	
Referans / Gerekçe	Kişisel Verilerin Korunması Kanunu ve Diğer Yasal Mevzuatlar
Onaylayan	Yönetim Kurulu

Değişiklik Tarihçesi			
Revizyon No	Tarih	Açıklama	Değişikliği Yapan

Dağıtım Listesi			
Doküman No	Birim	Kişi	Ünvan

İÇİNDEKİLER

1 AMAÇ

Bu politika, Şirket bünyesindeki bilgi sistemlerinin ve verilerin gizlilik, bütünlük ve erişilebilirliğini sağlayacak önlemlere ilişkin kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesi çalışmalarını gözetim altında tutmayı amaçlar.

2 KAPSAM

Bilgi, işle ilgili diğer önemli varlıklar gibi bir kuruluşun faaliyetleri açısından gerekli olan ve bunun neticesinde de uygun bir şekilde korunması gereken bir varlıktır. Bilgi varlıklarının güvenliği Şirket tarafından tanımlanmış politikalar doğrultusunda sağlanır. Bilgi güvenliğinin amacı; bilgiye yetkisiz erişimin engellenmesi (Gizlilik), bilginin ve bilgi varlıklarının tam ve eksiksiz olması, doğru olması ve uygunsuz biçimde değiştirilmemesi (Bütünlük) ve yetkili kullanıcıların ihtiyaç duydukları veriye ihtiyaç duydukları zaman erişebilmesinin (Erişilebilirlik) sağlanmasıdır.

Bilgi Güvenliği Politikası Şirket'in tüm birimlerine ve hizmet sağlayıcılarına uygulanır.

Şirket'in *Bilgi Güvenliği Yönetim Süreci*'nin hedefi Şirket tarafından üretilen, işlenen, saklanan bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak amacıyla bilgi varlıkları envanterini çıkarmak, risk değerlendirmesi yapmak, kontrolleri hayata geçirmek ve uygulanan kontrollerin etkinliklerini gözden geçirmektir.

3 TANIMLAR

Şirket: Pamukkale Kablo Sanayi ve Ticaret Anonim Şirketi (Pamukkale Kablo)

BT Verisi: Kullanıcıların sistemler üzerinde kimliklerini kanıtlamak amacı ile kullandıkları parola, PIN, şifreleme anahtarı, kart numarası, kişisel sertifika, akıllı kart gibi yüksek seviyede gizli sınıfındaki verileri

Bilgi Güvenliği ve Risk Komitesi: Bilgi sistemlerinin yönetimine ve bilgi güvenliğinin sağlanmasına ilişkin politikaların, prosedürlerin ve süreçlerin tesis edilmesi, bilgi teknolojilerinin kullanılmasından kaynaklanan risklerin etkin biçimde yönetilmesi amacıyla oluşturulan komiteyi temsil eder.

4 BİLGİ SİSTEMLERİ YÖNETİMİNE İLİŞKİN TEMEL İLKELER

- Bilgi sistemlerinin yapısının, Şirket'in ölçeği, faaliyetlerin ve sunulan ürünlerin niteliği, çeşitliliği ve stratejik hedefleri ile uyumlu olması; bilgi sistemleri ile içerdiği verinin güvenilir, doğru, eksiksiz, izlenebilir, tutarlı, erişilebilir ve ihtiyaçları karşılayacak nitelikte oluşturulması esastır. Bilgi sistemleri asgari olarak;

  - Şirket'le ilgili tüm bilgilerin yurt içinde elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanılmasına veya yedeklenmesine ve kullanılmasına,
  - Sızma ve stres testi yapılabilmesine,
  - Muhasebe kayıtlarının Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurulu tarafından belirlenen usul ve esaslara uygun şekilde muhasebeleştirilmesine

  imkân verecek yapıda tesis edilir.

- Bilgi sistemlerinin sürekli biçimde işlerliğini sağlamak üzere iş sürekliliği planı oluşturulur. Söz konusu planın işlerliği ve yeterliliği düzenli olarak test edilir; ihtiyaç duyulması halinde gerekli tedbirler alınır. İş sürekliliğinin planlanmasında, kritik bilgi teknolojileri varlıkları ile süreçleri belirlenir; bunlara ilişkin iş etki analizi ile risk değerlendirmesi yapılır.

- Bilgi sistemleri ile içerdiği verinin güvenli biçimde saklanması esastır. Bu çerçevede, veriler, güvenlik hassasiyet derecelerine göre sınıflandırılır, her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilir ve buna göre yedeklenir. Bilgi sistemlerinin güvenliği ve yedekleme sistemlerinin işleyişi düzenli olarak test edilir ve test sonuçlarına göre ihtiyaç duyulması halinde gerekli değişiklikler yapılır.

- Bilgi güvenliğinin temininde ve Şirket'in bilgi sistemlerine erişimde, kimlik doğrulama ve yetkilendirme mekanizmaları ile inkâr edilemezlik ve sorumluluk atama imkânlarını içeren teknikler kullanılır.

- Bilgi sistemlerinin geliştirilmesi, test edilmesi ve işletilmesi süreçlerinde görevler ayrılığı ilkesi uygulanır. Bilgi sistemleri yönetim sürecinde görev alan bölüm ve çalışanların görev, yetki ve sorumlulukları yazılı olarak belirlenir. Görevler ayrılığı ilkesine uygunluk düzenli olarak test edilir; sonuçları Bilgi Güvenliği ve Risk Komitesi'ne raporlanır.

- Faaliyetlerin yürütülmesi sırasında bilgi sistemleri aracılığıyla edinilen ve saklanan müşteri ve Şirket bilgilerinin gizliliğini sağlamak esastır. Müşteri bilgilerinin, yasalarla yetkili kılınmış merciler dışındaki taraflarla paylaşımına ilişkin uygulama esasları yazılı olarak belirlenir.

- Bilgi sistemleri kullanılarak gerçekleştirilen ve şirket faaliyetlerine ait kayıtlarda değişikliğe neden olan işlemlere ilişkin olarak yeterli detayda ve açıklıkta denetim izleri oluşturulur. Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli tedbirler alınır.

- Bilgi sistemleri yönetimi kapsamında alınacak Dış hizmetlerine ilişkin risk analizi yapılır.

- Uygulamaya konulan bilgi sistemlerinin işleyişi, stratejik hedeflere uygunluğu, kontrollerin etkinliği ve yeterliliği, bilgi teknolojilerindeki gelişmeler de göz önüne alınarak düzenli olarak izlenir. Yeni bilgi sistemlerinin Şirket'te uygulanmasının, Şirket'in risk profili üzerinde yaratacağı etki değerlendirilir. Bu çerçevede, gerek duyulması halinde, bilgi sistemleri işleyişi revize edilir.

5 BİLGİ GÜVENLİĞİ POLİTİKASI

Şirket *Bilgi Güvenliği Politikası* ile

- Kişisel bilginin mahremiyetinin korunmasını sağlamak amacıyla 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda belirtilen çerçeve içerisinde ilgili kişilerin bilgilerinin gizliliğini korur.
- Bilginin bütünlüğünü koruyacak ve sürekli erişilebilirliğini garanti altına alacak altyapıyı ve kontrolleri hayata geçirir.
- Tasarım, geliştirme, test ve uygulama süreçlerinde görevler ayrılığı prensibine uygun yetkilendirmeyi sağlar ve kritik işlemlerde onay mekanizması tesis eder.

- Geliştirme, Test ve Üretim ortamlarının fiziksel ve mantıksal olarak ayrılmasını sağlar
- Kullanıcıların yetkilendirilmesinde gerekli olan minimum yetkilendirme prensibinin sağlanması ve yetkilerin düzenli olarak kontrol edilmesini sağlar.
- Dış ağlardan gelebilecek tehditlere karşı ağ güvenliğini tesis eder.
- Katmanlı güvenlik mimarisini tesis eder ve sürekli gözetimini sağlar.
- Kullanılan şifreleme anahtarlarının güvenilirliğini sağlar.
- Mobil cihazlar üzerinde çalışan uygulamalar tarafından kullanılan hassas verilerinin güvenliğinin sağlanmasını (hassas verilerinin diğer uygulamalar tarafından kullanılamaması, kayıp/çalıntı durumunda erişilemez olması) tesis eder.
- Mobil cihazlar üzerinde çalışan uygulamaların güvenliğini sağlamaya önlemleri alır, gerekli güncellemeleri sağlar.
- Bilgi güvenliği faaliyetlerinin yönetilmesini ve koordinasyonunu sağlamak amacıyla bir bilgi güvenliği organizasyonu oluşturur.
- Bilgi varlıkları envanterini çıkarır, sahiplikleri belirler ve bilgi varlıkları üzerindeki riskleri yönetir.
- Bilgi güvenliği olaylarının tespit edilmesi, raporlanması ve tekrarının önlenmesi adımlarını içeren bilgi güvenliği olay yönetimi faaliyetleri gerçekleştirir.
- Tüm personele yeterli seviyede farkındalık programı uygular ve bilgi güvenliği gerekliliklerinin karşılanması için tüm çalışanların katılımını sağlar.
- Bilginin işlendiği alanlarda bilginin güvenliğinin sağlanabilmesi amacıyla gerekli fiziksel ve çevresel güvenlik önlemlerini alır.
- Bilgi sistemleri edinim, geliştirme ve bakımında güvenlik gerekliliklerinin neler olduğunu belirler ve hayata geçirir.
- Belirlenen bilgi güvenliği politikalarına, süreçlerine, yasal ve düzenleyici zorunluluklara çalışanların uymalarını yazılı taahhütlerini alarak zorunlu tutar.
- İş faaliyetlerindeki kesintileri önlemek ve bilgiye sürekli erişimi sağlamak için iş sürekliliği faaliyetleri gerçekleştirir.
- Bilgiye erişimi kontrol etmek ve yetkisiz erişimleri önlemek için ilgili tüm alanlarda gerekli güvenlik kontrollerini hayata geçirir.
- Bilgi sistemleri faaliyetlerinin işletilmesinde gerekli güvenlik kontrolleri uygular, buna yönelik rol ve sorumlulukları tanımlar.

6 BİLGİ GÜVENLİĞİ POLİTİKASININ ANA BAŞLIKLARI

6.1 BILGİ GÜVENLİĞİ ORGANİZASYONU

Şirket yönetimi bilgi güvenliği organizasyonunu Şirket bünyesinde oluşturur. Organizasyon Şirket'te güvenlik politikalarının bütünsel bir yaklaşımla oluşturulması, sürdürülmesi ve yönetilmesine ilişkin çalışmalarını yürütür

6.2 BİLGİ GÜVENLİĞİ ROL VE SORUMLUKLARI

Bilgi Güvenliğinin Şirket'te planlanması, uygulanması ve kontrol edilmesi faaliyetlerini gerçekleştirmek amacıyla, Bilgi Güvenliği ve Risk Komitesi, Bilgi Güvenliği Yetkilisi, Fiziksel Güvenlik Sorumlusu, Bilgi Varlıkları Sahipleri ve Şirket çalışanları görev alır. İlgili tarafların bu kapsamdaki görev ve sorumlulukları Bu politikaya ek olarak açık olarak tanımlanır.

Şirket *Bilgi Güvenliği Politikası* Bilgi Güvenliği Yetkilisi tarafından hazırlanır, Bilgi Güvenliği ve Risk Komitesi tarafından yılda en az bir defa gözden geçirilir ve Yönetim Kurulu tarafından onaylanır. *Bilgi Güvenliği Politikası* oluşturulurken Şirket'in güvenlik stratejisi, güvenlik gereksinimleri, yasal ve düzenleyici zorunluluklar göz önünde bulundurulur.

Şirket Üst Yönetimi *Bilgi Güvenliği Politikası*'nın hayata geçirilmesini sağlar.

6.3 BİLGİ VARLIKLARININ YÖNETİMİ

Basılı ve dijital ortamda oluşturulan, iletilen, saklanan veya sözlü olarak paylaşılan Şirket'e ait tüm veriler Şirket bilgi varlıkları kapsamına girer. Verinin iletilmesinde, işlenmesinde, erişilmesinde, saklanmasında, imhasında kullanılan uygulama, yazılım ve donanımlar da bilgi varlıkları kapsamına girer.

Şirket, bilgi varlıklarının ve bu veriyle ilgili tüm varlıkların gizliliğini, bütünlüğünü, erişilebilirliğini sağlayarak kazara veya kasti biçimde hasar görmesini, değişmesini, ifşa olmasını veya kaybolmasını önler. Bunun için varlık değerlendirmelerini yaparak bilgi varlıklarını sınıflandırır. Şirket bilgilerinin bu sınıflandırmaya uygun olarak kullanılmasını sağlar. Her varlığa bir sahip atanır ve varlıklarla ilgili sorumluluklar bu sahipler üzerine verilir.

6.4 RİSKLERİN DEĞERLENDİRİLMESİ

Şirket'in bilgi güvenliğine ilişkin risk değerlendirme yaklaşımı Bilgi Güvenliği ve Risk Komitesi tarafından belirlenir ve tanımlanır. Bilgi güvenliği risk değerlendirme yaklaşımı ile Şirket'in bilgi güvenliği risklerinin hangi yöntemler ile belirleneceği, risk seviyelerinin nasıl hesaplanacağı ve risklerin nasıl değerlendirileceği belirlenir. Bilgi varlıklarıyla ilgili oluşabilecek risklerin tanımlanması, derecelendirilmesi, işlenmesi ve gözden geçirilmesi çalışmaları belirlenen risk değerlendirme yaklaşımına uygun olarak gerçekleştirilir.

.

6.5 GÜVENLİK FARKINDALIĞI YARATILMASI

Şirket bütün personeli için farkındalık eğitim gerekliliklerini belirler ve personeline buna uygun bir şekilde eğitim sağlar. İşe yeni alınan her çalışanlar bilgi güvenliği konusunda bilgilendirilmelidir.

Şirket, kendi çalışanlarına ve tedarikçi şirket çalışanlarına bilgi güvenliği politikalarını bildiklerine ve uyacaklarına dair imzalı onaylarını alır.

6.6 FİZİKSEL VE ÇEVRESEL GÜVENLİK

Şirket *bu politikaya Ek İŞ SÜREKLİLİĞİ YÖNETİM PROSEDÜRÜ* kapsamında bilgi işleme faaliyetlerinin gerçekleştiği binalara, alanlara yetki dışı fiziksel erişimi, müdahale ve hasarı engellemek amacı ile fiziksel güvenlik önlemleri alır.

Bilgi işleme faaliyetlerinde kullanılan teçhizatlara yönelik güvenlik kontrolleri uygulanarak bilgi varlıklarının kaybı, hasarı, çalınması, tehlikeye girmesi ve kuruluşun faaliyetlerinin kesintiye uğraması engellenir.

6.7 HABERLEŞME VE İŞLETİM YÖNETİMİ

Bilginin işlendiği tesislerin, ortamların ve araçların amacına uygun ve güvenli bir şekilde işletilmesini ve yönetilmesini sağlamak amacıyla süreçler oluşturulur, sorumluluklar tanımlanır. Süreçlere yönelik sorumluluklar tanımlanırken bir işi yapan rol ile yapılan işi denetleyen rol aynı kişiye verilmez.

Yazılım ve bilginin bütünlüğünü korumak amacıyla kötü niyetli kodlara ve uygulamalara karşı güvenlik kontrolleri gerçekleştirilir.

Bilginin ve bilgi varlıklarının bütünlüğünü ve kullanılabilirliğini sağlamak için yedekleme faaliyetleri gerçekleştirilir. Ağdaki bilginin ve destekleyici altyapının korunmasını sağlanır.

Varlıkların yetkisiz ifşa edilmesi, değiştirilmesi, kaldırılması veya yok edilmesini ve iş faaliyetlerinin kesintiye uğramasını önlemek amacıyla bilginin işlenmesine, tedbirler alınır ve bunlar standart hale getirilir. Dış kurumlarla veya Şirket içerisinde alınıp verilen bilgi ve yazılımın güvenliğini sağlayacak güvenlik kontrolleri uygulanır.

İnternet sitesi hizmetlerinin güvenlik gereklilikleri sağlanır.

Yetkisiz bilgi işleme faaliyetlerini algılamak amacıyla bilgi sistemleri uygulamalarına yönelik denetim izleri oluşturulur ve izleme faaliyetleri gerçekleştirilir.

Yılda en az bir kere yetkin ve bağımsız bir dış şirket tarafından sızma testleri yapılır.

6.8 ERİŞİM KONTROLÜ

Bilgiye erişimi kontrol etmek için kullanıcı erişimleri güvenlik gereksinimlerini temel alacak şekilde yönetilir ve yetkisiz erişimler önlenir. Erişim yetkileri görevler ayrılığı ilkesine ve gerekli olan minimum yetkilendirme prensibine uygun olarak sağlanır. Yetkiler düzenli olarak gözden geçirilir.

Ağ erişimlerine yönelik güvenlik kontrolleri ile ağ bağlantılı hizmetlere yetkisiz erişimler engellenir. İşletim sistemlerine ve uygulamalara yönelik erişim kontrolleri hayata geçirilir. Mobil bilgi işleme ve uzaktan çalışma hizmetlerini kullananlar için bilgi güvenliği gereksinimleri karşılanır.

6.9 AĞ GÜVENLİĞİ

Ağ trafiğinde güvenliği sağlamak amacıyla, ağ kontrol güvenlik sistemleri bulunur. Ağ güvenliğinde dış güvenlik duvarı, IPS, iç güvenlik duvarı, SSM gibi katmanlı güvenlik mimarisi (bir güvenlik katmanının aşılması durumunda diğer güvenlik katmanının devreye girdiği) kullanılır. Ağ güvenliğinde kullanılan sistemler, sürekli gözetim altında tutulur. Dış ağ ile kurulan bağlantılarda VPN ve SSL kullanılır.

6.10 BİLGİ SİSTEMLERİ EDİNİM, GELİŞTİRME VE BAKIMI

Gerçekleştirilen bilgi sistemleri edinim, geliştirme ve bakımı operasyonlarında güvenlik gereksinimleri uygulanır. Uygulamalardaki bilginin bozulmasının, kaybının, yetkisiz değiştirilmesinin ve kötüye kullanımının önlenmesi için kontroller hayata geçirilir. Gerektiği durumlarda bilginin gizliliğini ve bütünlüğünü sağlayacak kriptografik uygulanır. Sistem dosyalarının ve sistem verilerinin güvenliğini

sağlamak amacıyla güvenlik kontrolleri uygulanır.

Uygulamalar ve sistemler üzerinde yapılacak değişiklikler ile kontrollü olarak gerçekleştirilir ve güvenlik riskleri azaltılır. Dışarıdan sağlanan yazılım geliştirmelerinin bilgi güvenliği gereksinimlerini sağlaması temin edilir.

6.11 BİLGİ GÜVENLİĞİ OLAYLARI YÖNETİMİ

Bilgi sistemleri ile ilişkili bilgi güvenliği olayları, ihlalleri ve zayıflıkları *bu politikaya ek olarak belirlenecek kanallardan* raporlanır. Raporlama düzeltici önlemlerin zamanında alınabilmesini sağlayacak şekilde gerçekleştirilir. Tüm çalışanların, tedarikçilerin ve üçüncü taraf kullanıcıların bilgi güvenliği olaylarının raporlanmasına katılımı sağlanır. Olayların sonucunda iyileştirici faaliyetler hayata geçirilir tekrar eden olayların önüne geçilir.

6.12 BILGI SISTEMLERI SÜREKLİLİĞİ YÖNETİMİ

İş faaliyetlerindeki kesilmeleri önlemek, önemli iş süreçlerini bilgi sistemleri aksaklıklarından korumak için bilgi sürekliliği faaliyetleri gerçekleştirilir. Bu faaliyetlerin bilgi güvenliği gereksinimlerini karşılaması sağlanır.

6.13 UYUM

Tüm Şirket çalışanları, ilgili yasalar, yönetmelikler ve sözleşmelerden doğan güvenlik gereksinimlerine, fikri mülkiyet haklarına, lisans anlaşmalarına ve Şirket tarafından belirlenen güvenlik gereksinimlerine uymakla yükümlüdürler. Yöneticiler sorumluluk alanlarındaki tüm süreçlerin işletilmesinde güvenlik politikalarına ve standartlara uyumu temin eder. Tüm Şirket çalışanları, Şirket verilerinin gizlilik derecelerine uygun şekilde kullanımı konusunda sorumludurlar.

Şirket'in bilgi güvenliği politikalarına uyumun denetlenmesi için bilgi güvenliği gözden geçirme faaliyetleri gerçekleştirilir. *Bilgi Güvenliği Politikası'*na uyum durumu yılda en az bir defa yönetim kuruluna raporlanır.

7 BİLGİ GÜVENLİĞİ POLİTİKASININ GÖZDEN GEÇİRİLMESİ

Şirket *Bilgi Güvenliği Politikası* Bilgi Güvenliği Yetkilisi tarafından yılda en az bir kere gözden geçirilir ve gerekli görülmesi durumunda güncellenerek Yönetim Kurulu onayına sunulur. Güvenlik teknolojilerindeki gelişmelere bağlı olarak ortaya çıkan ihtiyaçları içerecek yeni politikalar üretilir.

8 BİLGİ GÜVENLİĞİ POLİTİKASININ UYGULAMA SORUMLULUĞU

Tüm çalışanların *Bilgi Güvenliği Politikası*'ndan haberdar olması sağlanır. Politikanın son hali tüm personele duyurulur ve personelin sürekli olarak erişebileceği ortak bir alanda yayımlanır. Personel kendisini ilgilendiren genel hükümlere uymak zorundadır. Personelin kendisini ilgilendiren genel hükümlere uyup uymadığının kontrol edilmesi sorumluluğu personelin idari amirindedir. Bilgi güvenliği politikalarına uyum düzenli olarak izlenir.

9 YÜRÜRLÜK

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

EKLER

Ek No	Ek Adı	Ek Açıklaması
PK-PR11	**DÜZELTİCİ FAALİYETLER PROSEDÜRÜ**	Düzeltici Faaliyetleri planlamak, uygulamak, yürütmek ve kontrol etmek, etkinliğini ölçmek, hataya yol açan konuların ortadan kaldırmak ve sorumluları belirlemek.
PK-PR50	**BGYS KAPSAM VE BAĞLAM PROSEDÜRÜ**	
PK-PR51	**VARLIK ENVANTERİ PROSEDÜRÜ**	
PK-PR52	**BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ PROSEDÜRÜ**	
PK-PR53	**DİSİPLİN PROSEDÜRÜ**	
PK-PR54	**İŞ SÜREKLİLİĞİ YÖNETİM PROSEDÜRÜ**	
PK-PR55	**İŞLETİM PROSEDÜRÜ**	
PK-PR56	**BİLGİ GÜVENLİĞİ RİSK YÖNETİMİ PROSEDÜRÜ**	
PK-PR57	**İŞE ALIM VE İSTİHDAMIN SONA ERMESİ PROSEDÜRÜ**	
PK-PR59	**OLAY RAPORLAMA VE YÖNETİM PROSEDÜRÜ**	
PK-PR60	**ACİL DURUM EYLEM PROSEDÜRÜ**	