SİTEPLUS ÖZEL GÜVENLİK HİZMETLERİ A.Ş.

2020

BİLGİ GÜVENLİĞİ POLİTİKASI

KVKK_P5 VERSİYON 1.00

SİTEPLUS ÖZEL GÜVENLİK HİZMETLERİ A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç:

Bilgi, SİTEPLUS Özel Güvenlik Hizmetleri A.Ş.'nin tüm faaliyetlerinin desteklemesi noktasında temel bir rol oynamaktadır. Şirketimizin işlediği tüm bilgileri uygun şekilde güvence altına almak, ekonomik ve idari faaliyetlerinin başarısı için gereklidir. Bu hedefe bilgi güvenliğinin üç temel özelliği ele alınarak ulaşılması ön görülmektedir: Şirketin bilgilerini korumak için hayati yapı taşları olan veri gizliliği, veri bütünlüğü ve verilere ulaşım/kullanılabilirlik.

İşbu Politikanın amaçları aşağıda sıralandığı gibidir:

1.1. Şirketin bilgi kaynaklarını kayıp, kötüye kullanım ve ihlal durumlarına karşı yeterli düzeyde bir korunma sağlamak;

1.2. Tüm kullanıcılarının işbu Politika ve ilgili diğer politika metinleri, davranış kuralları ve kılavuzlar hakkında bilgi sahibi olmalarını temin etmek;

1.3. Tüm kullanıcıların ilgili yürürlükteki Türk hukuku ve bu bağlamda mükellef oldukları sorumluluklar hakkında bilgi sahibi olmalarını temin etmek;

1.4. Bilgi güvenliğinin etkin bir şekilde işletilmesi ve desteklenmesi amacının bir parçası olarak Şirket genelinde uygun güvenlik önlemlerinin uygulanması gerektiğine dair çalışanlar ve diğer paydaşlar arasında farkındalık yaratmak;

1.5. Tüm kullanıcıların işlemekte oldukları verilerin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması noktasında üzerlerine düşen sorumluluklar hususunda bilgi sahibi olmalarını temin etmek;

İşbu Politikanın kişisel verilerin korunması konusunda ayrıntılı bilgilere yer veren SİTEPLUS Özel Güvenlik Hizmetleri A.Ş. Kişisel Verilerin İşlenmesi ve Korunması Politikası ve ilgili uygulama esasları ile birlikte ele alınması gerekir.

2. KAPSAM:

İşbu politika Şirket bünyesinde yapılan ticari faaliyetlere ve bu işlemlere ilişkin lojistik, depolama, muhasebe, finans, kalite güvence, satın alma, insan kaynakları, hukuk, satış, pazarlama, iç denetim ve bilgi işlem faaliyetlerinden elde edilen elektronik bilgi varlıkların korunması, SİTEPLUS Özel Güvenlik Hizmetleri A.Ş. bünyesinde tutulan kişisel verilerin kanun kapsamında işlenmesi, saklanması, korunması, gizliliğinin ve bütünlüğünün bozulmaması için kullandığı bilgi güvenliği süreçlerini kapsar.

2.1. Tüm Şirket çalışanları ve Şirket tarafından ya da Şirket nam ve hesabına kontrol edilmekte olan bilgilere erişmelerine izin verilen misafirler de dâhil olmak üzere diğer

tüm ilgili üçüncü taraflar işbu belgede serdedilen Bilgi Güvenliği Politikası ve bununla ilintili uygulama esaslarına uymakla mükelleftir. İşbu Politika hükümleri, yukarıda zikredilen tarafların, hem Şirket nezdinde hem de Şirket dışı sistemler üzerinden Şirket'in sahip olduğu / kiraladığı ve/veya ödünç verilen cihazları ve tüm sair Şirket harici temin edilen araç ve sistemleri kullanmak suretiyle SITEPLUS Özel Güvenlik Hizmetleri A.Ş.'nin sunduğu ağlara doğrudan ya da dolaylı olarak bağlanarak Şirkete ait ya da Şirketin kullanımı için lisanslanmış tüm veri ve yazılımlara erişimleri ve kullanımları süreçlerini kapsamaktadır.

2.2. İşbu Politika aşağıda sıralanan yöntemler de dâhil olmak üzere Şirket tarafından elektronik ya da fiziki ortamda tutulan tüm veriler için geçerlidir:

- Masaüstü ve diz üstü bilgisayar ve sair cihazlar ile depolama cihazları tarafından depolanan ve işlenen elektronik veriler;
- Ağ ortamları üzerinden aktarılan veriler;
- Faks ve benzeri aktarım yöntemle kullanılarak gönderilen bilgiler;
- Tüm kâğıt ortamında tutulan kayıtlar;
- Mikrofiş, slayt ve CCTV kayıtları dâhil olmak üzere görsel ve fotoğrafik materyaller; yüz yüze iletişim dâhil olmak üzere sesli mesaj ve kaydedilen konuşmalara ilişkin sesli veriler;

2.3. Şirket verileri genel olarak kişisel veriler ve kişisel olmayan veriler olarak sınıflandırılabilir:

- Kişisel veriler Şirketin Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak işlenmekte olup en yüksek koruma standardına tabidir;
- Kişisel olmayan veriler ise aşağıdaki veri çeşitlerini içermektedir:
  i. Ticari olarak hassas kabul edilen planlama verileri, araştırma ve verileri, gizlilik sözleşmeleri ile korunan veriler ile kanunen imtiyazlı ya da gizli olduğu öngörülen veriler dâhil olmak üzere özel nitelikli Şirket verileri. Bu kategorideki veriler yüksek düzeyde korumaya tabidir.
  ii. Şirketin kurumsal web sitesinde yayımlanarak kamuya açıklanan ya da Bilgi Edinme Kanunu gibi yasal düzenlemeler doğrultusunda kamuya açıklanabilecek olan diğer Şirket verileri. Bu veri kategorideki verilerin içeriğinin doğru ve güncel olması ve kayıp ile yetkisiz müdahalelere karşı korunması esastır.

2.4. İşbu Politika hükümleri verilerin toplanması, depolanması, işlenmesi ve imhası da dâhil olmak üzere tüm yaşam döngüsü aşamaları için geçerlidir.

2.5. Her ne kadar sosyal medya ortamlarının çalışanlarımız tarafından kullanımı serbest ve doğrudan Şirket tarafından düzenlenmemekte ise de Şirketimiz çalışanlarının işbu Politika hükümlerine riayet etmesini ve Şirketin kurumsal itibarını zedeleyecek davranışlardan kaçınmasını şart koşmaktadır. Bu konuda ayrıntılı bilgi için Sosyal Medya Politikası incelenmelidir.

3. SORUMLULUK VE YETKİ:

Sorumluluk ve yetkileri belirlenmiş çalışanların nitelik ve yeterlilikleri görev tanımlarında tanımlanmıştır. Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesi ve geliştirilmesi bakımından ilgili birim ve görevlilerin sorumlulukları ise aşağıdaki gibidir:

3.1. Departman Sorumluları ve Şube Müdürleri

Departman Sorumluları ve Şube Müdürleri departman ve şubelerde istihdam edilen personel ve yetkilendirilmiş diğer kişilerin özellikle de IT Kaynaklarının Kullanım Koşulları altında zikredilen usul ve esaslara uygun hareket etmelerini temin etmekle mükelleftirler. Aynı zamanda sorumlu oldukları birimler tarafından tutulan bilgi kaynaklarının Şirketin Bilgi Kaynakları Envanterine kaydedilmesi ve her bir bilgi kaynağı için Bilgi Kaynağı Kullanıcısı atamakla görevlidirler.

3.2. Bilgi Kaynağı Kullanıcıları

Bilgi Kaynağı Kullanıcıları, Şirketin Bilgi Kaynakları Envanterinde listelenen bilgi kaynaklarının her biri için atanan sorumlu kullanıcılardır. Bahse konu kullanıcılar sorumlu oldukları bilgi kaynaklarının güvenlik ve gizliliklerine ilişkin riskleri yıllık olarak değerlendirmek suretiyle Veri Koruması Risk Değerlendirmesi yapmak ve uygun uygulama tedbirleri almakla görevlidirler.

3.3. Çalışanlarımız ve yetkilendirilen üçüncü taraflar

Tüm Şirket çalışanları ve Şirket tarafından bilgi kaynaklarına erişmek için yetkilendirilen tüm üçüncü taraflar işbu Politika metninde belirtilen hususlara riayet etmekle mükelleftirler. IT Kaynaklarının Kullanım Koşulları bağlamında kendilerine tahsis edilen kullanıcı adlarını kullanmaya başlamadan önce tüm çalışanların ekranında görünecek olup bahse konu başlık altında belirtilen koşulların kabul edilmesi zorunludur. Kaza eseri verilerin ifşa olması ya da kaybolması, yetkisiz erişim, bilgisayar virüsü, kötü amaçlı yazılım gibi bilgi güvenliğini ihlal edecek olaylarla karşılaşılması ya da bundan şüphelenilmesi durumunda derhal IT Departmanına durum raporlanmalıdır. İlgili kişiler IT Departmanının yönetici ya da çalışanlarıyla bu amaçla doğrudan iletişime geçebilirler. (İrtibat bilgileri için bkz. Bölüm 7.1)

3.4. IT Departmanı Sorumlusu

IT Departmanı Sorumlusu, bilgi ve iletişim teknolojileri kaynaklarının kontrolü ve günlük bilgi güvenliği faaliyetlerinin gerçekleştirilmesinden sorumludur. IT Departmanı Sorumlusu, Güvenlik risklerinin tespiti ve zararlarının giderilmesi ve/veya azaltılması amacıyla kullanılan tüm sistemleri denetleyebilir ya da ağ üzerinde yer alan sistemlerde bulunan güvenli olmadığı değerlendirilen kullanıcı/oturum açma adı, veri ve/veya programları kaldırabilir ya da erişilemez kılabilir.

4. YÜRÜRLÜKTEKİ MEVZUATA UYUM

4.1. SITEPLUS Özel Güvenlik Hizmetleri A.Ş. yürürlükteki tüm Türk kanunları ve idari düzenlemelerine riayet etmekle mükelleftir. Bilgi güvenliği bakımından ise 5651 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği başta gelen mevzuat unsurlarıdır.

4.2. Yukarıda zikredilen mevzuat hükümlerine uygun hareket etmek tüm kullanıcılar açısından geçerli bir sorumluluk olup aykırı davranış durumunda bireysel sorumluluk söz konusu olabilecektir. Her bir çalışanın işbu Politika ya da yürürlükteki mevzuat hükümlerine aykırı hareket etmesi halinde Şirketimizle imzalanan iş akdi ilgili ve Disiplin Yönetmeliğinde düzenlenen ilgili disiplin işlemleri başlatılabilir. Tedarikçi ya da üstlenici paydaşlarımızın aykırı davranışları ise tarafımızla akdedilen sözleşmenin feshine neden olabilir. Bazı durumlarda ise yasal işlem yapılması söz konusu olabilir.

5. ŞİRKET VERİ ENVANTERİ VE VERİ KORUMASI ETKİ DEĞERLENDİRMESİ

5.1. SITEPLUS Özel Güvenlik Hizmetleri A.Ş. bünyesinde kullanılan veri kaynakları ile ilgili detayların yer aldığı bir Veri Envanteri tutmaktadır. Departman Sorumluları ve Şube Müdürleri sorumlu oldukları birimlerce tutulan her bir bilgi kaynağı için Kaynak Kullanıcısı atamak ve bu hususu Şirket Veri Envanterine kaydetmekten sorumludur.

5.2. Yıllık olarak tüm kullanılan bilgi kaynakları için veri gizliliği ve güvenliğine ilişkin riskler ve kullanılan araçların kişilerin özel hayatın gizliliği hakkı bakımından doğuracağı riskler hususunda bir etki değerlendirilmesi yapılacaktır. Etki değerlendirmesi ayrıca yeni bilgi kaynakları kullanılmadan önce de icra edilecektir. Özel nitelikli veri olarak tanımlanan verilerin işlendiği kaynaklar için söz konusu riskleri azaltmak için alınması kararlaştırılan tedbirler veri envanterinde belirtilecektir.

6. ELEKTORNİK HABERLEŞMELERİN DENETLENMESİ

5561 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun Erişim sağlayıcının yükümlülükleri başlıklı 6. Maddesi gereği Şirket, kanunda sayılan amaçlarla sınırlı olarak Şirket tarafından alınan ya da gönderilen elektronik haberleşme trafik bilgilerini saklamak, bu bilgilerin doğruluğu, bütünlüğü ve gizliliğini sağlamak için gerekli tedbirleri alacaktır. Bahse konu amaçlara suç teşkil eden ya da izin verilmeyen amaçla için kullanılıp kullanılmadığını kontrol etmek, virüsler, hackleme ve hizmeti engelleme saldırısı (denial of service attack) gibi tehditlere karşı sistemin korunmasına yönelik denetleme ve müdahaleler, bilgi işlem operasyonlarının Şirketin politika ve direktiflerine uygunluğunu temin etek dâhil ancak bunlarla sınırlı değildir. Denetleme İşlemleri Elektronik Haberleşme ve Verilerin İncelenmesi Hakkında Uygulama Esaslarına Uygun olarak yerine getirilecektir.

7. VERİ GÜVENLİĞİNİ İLGİLENDİREN OLAYLAR

7.1. Herhangi bir kullanıcı veri gizliliği, erişebilirlik ve bütünlüğünü ihlal eden veri güvenliği ihlalini ya da bilgi kaynaklarının kötüye kullanımını tespit eder ya da ihlal durumunun muhtemel olduğunu düşünürse IT Departmanı Destek Ekibini bilgilendirecektir.

7.2. Eğer veri güvenliği ihlali kişisel verilerin kazara ya da kanuna aykırı olarak imhası, kaybı, değiştirilmesi, kişisel verilere etkisiz erişim ya da kişisel verilerin yetkili olmayan taraflara ifşasını içeriyorsa kullanıcılar derhal Veri İhlali Müdahale Planı'nın ekinde yer alan Veri Güvenliği İhlali Bildirim Raporunu düzenleyerek Veri koruma İrtibat Görevlisi/Sorumlusuna gönderecektir.

Veri Koruma İrtibat Görevlisi/Sorumlusu İrtibat Bilgileri:
SITEPLUS Özel Güvenlik Hizmetleri A.Ş.
Telefon: (312) 236 12 56
Faks: +90 312 236 23 42
Elektronik Posta: siteplusguvenlik@hs01.kep.tr

7.3. Bir veri güvenliğini ilgilendiren olayın gerçekleşmesi ya da gerçekleşmesinden şüphe edildiği durumlarda IT Departman Sorumlusu, olayın bertaraf edilmesi ya da doğacak zararların azaltılması için gerekli olduğunu düşündüğü kullanıcıların sisteme erişimini engellemek ya da ağa bağlı olan cihazları incelemek gibi tedbirleri ivedilikle alabilir.

7.4. Veri güvenliğini ilgilendiren bir olayı ya da kişisel veri ihlalini rapor etmekten imtina edilmesi durumunda disiplin yönetmeliğine göre soruşturma açılabilir. Herhangi bir olayı rapor etmede tereddüt yaşanması halinde IT Departman Sorumlusu ya da Veri Koruma İrtibat Görevlisi/Sorumlusundan görüş alınabilir.

8. VERİ GÜVENLİĞİ EĞİTİMLERİ

8.1. IT cihazlarını ilk defa kullanacak olan çalışanlar ve cihazlara erişimi onaylanan üçüncü tarafların Şirketin bilgi güvenliğine ilişkin politikaları ve uygulama esasları hakkında bilgi sahibi olmaları sağlanmalıdır. Ayrıca IT hizmetlerine erişim izni verilmeden önce, üstlenecekleri işin güvenlik gereksinimleri ile ilgili prosedürler ve genel olarak Şirket'in BT varlıklarının doğru kullanımı konusunda kullanıcılara eğitim verilmelidir. Çalışanlarının uygun şekilde eğitilmesi ve eğitim kayıtlarının tutulması yöneticilerin sorumluluğundadır. Bölüm 7'deki raporlama prosedürleri dâhil olmak üzere, kullanıcılar işbu Politika hakkında bilgilendirilmelidirler.

8.2. Şirketin tüm çalışanları çevrim içi ya da yüz yüze gerçekleştirilecek olan bilgi güvenliği farkındalık eğitimleri ve kişisel verilerin korunması eğitimlerine tabi tutulacaklardır. Bahse konu eğitimlerin ileride zorunlu kılınması planlanmaktadır.

9. İSTİHDAM ALANINDA GÜVENLİK DEĞERLENDİRMELERİ

9.1. Bu politikada ve ilgili Uygulama Kurallarında belirtilen güvenlik konusunda üstlenilecek roller ve sorumlulukları, uygun olduğu yerlerde iş tanımlarına dâhil edilmelidir. Bunlar, güvenlik politikasının uygulanmasına yönelik genel sorumlulukların yanı sıra belirli bilgi varlıkların korunması veya güvenlik süreçleri veya faaliyetlerinin yürütülmesine yönelik sorumlulukları da içermelidir.

9.2. İş başvuruları ya da çalışanların görev değişimi durumlarında veri güvenliği konusunda tanınan yetki ve sorumluluklar da değişim olabileceği için bu hususlar İnsan Kaynakları tarafından değerlendirilmelidir.

9.3. Şirketin bilgi sistemlerini kullanacak tedarikçi ya da üstlenici firma çalışanları ve üçüncü taraf kullanıcılarının kendileriyle akdedilen sözleşmelerin bir parçası olarak gizlilik sözleşmeleri imzalamaları ve Şirketin muhafaza ettiği kişisel verilere erişimleri söz konusu olması halinde ise Veri paylaşma Sözleşmelerini imzalamaları talep edilecektir.

10.ÖZEL NİTELİKLİ VERİLERİN KORUNMASI

10.1. Şirketin özel nitelikli verilerin korunması için daha güçlü güvenlik tedbirleri uygulaması esastır.

10.2. Özel nitelikli veriler Şirket tarafından tedarik edilmeyen bireysel elektronik posta (Gmail, Hotmail vb.) ya da web tabanlı "bulut" depolama servisleri (Google Apps, Dropbox vb.) ortamlarda depolanmamalı ve bu ortamlar kullanılarak aktarılmamalıdır.

10.3. Özel nitelikli veriler ihtiva eden veri tabanları ve bilgisayarlar şifrelenmeli ve kullanıcıların verilere erişmek için kimlik bilgilerini girmesini gerektirmelidir. Mümkün olduğunda, özellikle hasta / katılımcının tanımlanabilir verilerinin söz konusu olduğu durumlarda, veriler anonim hale getirilmeli veya takma ad kullanılarak kimlik bilgilerinin korunması sağlanmalıdır.

10.4. Şirketim kullandığı tüm cihazlar elden çıkarılırken güvenli bir şekilde verileri silinmelidir.

10.5. Veri dosyaları hem muhafaza edildikleri ortamlarda hem de aktarılırken şifrelenmelidir.