ONCOSEM ONKOLOJİK SİSTEMLER SAN. VE TİC. A.Ş.

BİLGİ SİSTEMLERİ YÖNETİMİ POLİTİKASI

Bu politika,

ONCOSEM ONKOLOJİK SİSTEMLER SAN. VE TİC. A.Ş. 'nin bilgi varlıklarının iş sürekliliğinin sağlanması, bu bilgi varlıklarına yönelik risklerin yönetilmesi ve bilgi varlıklarının iş amaçlarına uygun kullanılması için gerekli kuralları ve yaklaşımlarımızı tanımlar.

Şirket faaliyetlerimizi gerçekleştirirken bilginin alınması, oluşturulması, işlenmesi, aktarılması tutulması, arşivlenmesi ile ilgili yapılacak çalışmalarda bilgi varlıklarımızın gizlilik, güvenlik ve bütünlüğünü koruyacak şekilde Bilgi Güvenliği Yönetim Sistemi (BGYS)'nin ISO 27001 standardının gereklerini yerine getirecek şekilde kurulması, yönetilmesi ve sürekli iyileştirilmesi amaçlanmıştır.

Bu politika, Şirketimizin tüm birimlerini, çalışanlarımızı ve müşterilerimizi kapsamaktadır. Çalışanlarımız (Kullanıcı) bu politikanın ekinde belirtilen kurallara, süreç ve talimatlara uymakla yükümlüdürler ve bu politikayı okuyarak işbu Politika 'da tanımlanan kurallara uymayı taahhüt etmiş olurlar. Çalışanlarımıza, bilgi güvenliği farkındalığını artırmak amacıyla teknik ve davranışsal yetkinliklerini geliştirecek şekilde eğitimler gerçekleştirilecektir.

Bilgi güvenliği yönetim sistemi kapsamı dâhilindeki bilginin gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik bir çerçeveyi tanımlamak.

Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmek.

Tabi olduğu ulusal veya sektörel düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.

Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak.

Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmak.

Kurum itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak.

BGYS, sürekli ve sistematik olarak değerlendirilecek ve geliştirilecektir. Sistemin kurulmasından, sürekli geliştirilmesi ve kontrolünden **Bilgi Güvenlik Yönetim Sistemi Yöneticisi** sorumludur.

Bilgi güvenliği ile ilgili tüm yasal mevzuat ve sözleşmelere uyulacaktır. Şirketimizin bilgi güvenliği riskleri "Risk Yönetimi Süreci' ne göre tanımlanmış olup; işbu politika Sistematik olarak gözden geçirilecektir.

Bilgi Güvenliği Politikası' nın en etkili şekilde uygulanacağını; Bilgi Güvenliği Yönetim Sistemi'ni diğer yönetim sistemlerimizle bütünleşik şekilde yöneterek sürekli geliştirileceğini ve kontrol edileceğini; güvenlik ihlallerinde gerekli yaptırımların uygulanacağını taahhüt ederiz.

ONCOSEM ONKOLOJİK SİSTEMLER SAN. VE TİC. A.Ş.

1. GENEL KURALLAR

Çalışanlar, ONCOSEM A.Ş. 'in Bilgi Güvenliği Yönetim Sistemi (BGYS) ISO 27001 Standardı gereği işbu Bilgi Güvenlik Politikasına, ONCOSEM A.Ş. Personel Yönetmeliği'ne, Disiplin Yönetmeliği'ne, Bilgi Güvenlik Politikasında atıf yapılan veya bahsi geçen tüm prosedürlere, talimatlara, mevzuata ve işbu taahhütname şartlarına uymayı, ve görevlerine ilişkin bilgi ve belgelerin gizliliğini korumayı taahhüt ederler. Her ONCOSEM A.Ş. çalışanı bilgi gizliliğini korumakla sorumludur ve "**Personel Bilgilendirme Forumu**'nu imzalar.

Şirket çalışanları, gerçekleştirdikleri çalışmalar sonucunda oluşturdukları her türlü bilgi, dosya ve/veya programın saklanması/muhafazası ve fiziksel güvenliğinin sağlanmasından sorumludurlar.

Elektronik Bilgiler:

- Şirket çalışanları kendi bilgisayarları üzerinde yer alan değerli ve kritik bilgilerinin Ortak Kullanım Sunucusu üzerinde güvenli olarak yedeklenmesinden Sorumludurlar. Bu nedenle, çalışanlar tarafından işle ilgili değerli ve kritik bilgiler, kişisel bilgisayarlarda muhafaza edilmek yerine, Ortak Kullanım Sunucusu içinde çalışan için ayrılmış "Paylaşımlı" ve "Özel" isimli çalışma dosyalarında muhafaza edilecektir.
- Şirket tarafından tahsis edilmiş kişisel bilgisayarlar ve Ortak Kullanım Sunucusu üzerinde kullanıcının izni ve yetkisi dışındaki belge, bilgi veya yazılım alışverişinde bulunulmayacaktır.
- Yetkisi olmayan çalışanın, Şirket'in gizli ve hassas bilgilerini görmesi veya elde etmesi yasaktır. Bu nedenle, kişisel bilgisayarlar üzerinde problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmeyecektir ve karşılaşılan sorunlar yetkili kişilere bildirilecektir.
- Ortak Kullanım Alanların 'da gereksiz yer kaplayacak ve iş ile ilgili olmayan müzik ve resim dosyaları, oyunlar, filmler ve benzeri programların (mpg, mpeg, avi, exe, com, gif, jpg uzantılı dosyalar) bulundurulması yasaktır.

Kağıt Ortamındaki Bilgiler:

- Hassas olsun veya olmasın, çalışanların görevlerine ilişkin bilgi ve belgelerin gizliliği korunacak, bilgi ve belge niteliğindeki kâğıt ortamdaki dokümanlar, "**Back Up Kullanma Talimatı"**'na göre kayıt altına alınacaktır.

- Şirket çalışanları mesai saatleri dışında ve izinli olduğu dönemlerde masalarının üzerinde Şirkete ait hassas olsun olmasın hiçbir belgeyi açıkta bırakmayacaktır.
- Hassas bilgileri içeren kâğıt ve elektronik depolama ortamları kullanılmadığı zaman kilitli dolap ve/veya kasa içinde korunacaktır.

Bilgi ve Haberleşme Sistemleri ve Donanımları:

- İnternet, ortak kullanım sunucuları, e-posta, telefon, çağrı cihazları, faks, bilgisayarlar, mobil cihazlar ve cep telefonları da dahil olmak üzere **Şirket Varlık Yönetimi Süreci** uyarınca yönetilirler.
- Şirket telekomünikasyon cihazları kullanılırken ilgili yasa ve düzenlemelere uyulur.
- Şirket için veya Şirket adına alınmış olan, Şirket çalışanları veya ilgili kişiler tarafından Şirket için geliştirilmiş olan tüm donanımlar Şirket'in malıdır. Tüm donanımlar, ilgili lisans, uyarı, sözleşme ve anlaşmalar uyarınca kullanılacaktır.
- Şirketin bilgi ve haberleşme sistemleri ve donanımları öncelikli olarak Şirket işlerinin gerçekleştirilmesi için kullanılır. Şirket çıkarlarıyla çakışmadığı ve kullanım miktarları Şirketi maddi zarara uğratmayacak limitler dahilinde kullanıldığı sürece telekomünikasyon cihazlarının kişisel kullanımına izin verilir. Ancak, Şirketin normal operasyon ve iş aktivitelerini engelleyemez. Kişisel kullanımlarda aşırılık tespit edildiği durumlarda Şirket telekomünikasyon cihazının kullanımını kısıtlama ve iptal hakkını saklı tutar.
- Kullanıcılar telekomünikasyon cihazları ile yaptıkları tüm iletişimden sorumludur.
- Şirket telekomünikasyon cihazlarını hiçbir şekilde yasa dışı kullanılamaz. Şirket telekomünikasyon cihazlarını uygunsuz içeriği saklamak, erişmek, indirmek ve iletmek için kullanılamaz. Kullanıcıların telekomünikasyon cihazlarını kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır. Ayrıca bilgi, zararlı yazılımlara karşı taramadan geçirilmeden Şirket ağına aktarılamaz.
- Bu sistemlerin yasa dışı, rahatsız edici, Şirketin diğer politika, standart ve rehberlerine aykırı veya Şirkete zarar verecek herhangi bir şekilde kullanımı, bu politikanın ihlal edildiği anlamına gelir.

2. PAROLA KULLANIMI VE UZAKTAN SİSTEME ERİŞİM KURALLARI

Şirket çalışanlarının gerçekleştirdikleri çalışmalar için kullanımlarına verilmiş masa üstü bilgisayarlar,notebooklar ve/veya mobil cihazlar üzerinden Şirket bilgisayar ağına erişmeleri sağlanmaktadır. Bilgi kaynaklarına erişim **“Şifre Talimatı”** ve **“Uzaktan Erişim Talimatı”**na uygun olarak gerçekleştirilecektir.

- Uzaktan erişim, çalışanlara verilen “Kullanıcı Hesapları (User Account)” ile sağlanmaktadır.
- Sunucular ve ağ cihazları da dahil olmak üzere erişim kontrolünün sağlanması ve yetkisiz erişimin engellenmesi amacıyla her “Kullanıcı Hesabı” için kullanıcı adı ve parola verilmektedir.
- Her türlü kullanıcı şifresi çalışanın sorumluluğundadır.
- Çalışanlar kendilerine verilen kullanıcı adı ve parolaları kullanırken kendilerine duyurulan “Parola Kullanım ve Yönetim Talimatına uyacaklardır.

- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmayacaktır, kaynakların paylaşıma açılması halinde de mutlaka “Parola Kullanım ve Yönetim Talimatı’ kurallarına göre hareket edilecektir.
- Çalışanlar, IT departmanı bilgisi dışında uzaktan erişimle bağlanamaz, bağlanırken ve bağlantıyı keserken bilgi verir, çalışırken işiyle ilgili olmayan dosyalara giremez. Yapılan uzaktan erişimlerin tamamı kayıt altında tutulacaktır.
- İnsan Kaynakları ile ilgili yazılımlara (PDKS), veri tabanına ve dosyalara İK’nın bilgisi ve izni dışında ulaşılamaz. İK ile ilgili yazılımlar ve veri tabanında ADMİN kullanıcı, İK Müdürü’dür. Loglar ise Bilgi İşlem Bölümü’ne açıktır.
- Kullanıcılar, kendilerine erişim izni verilmiş olan bilgiler ve alanlar dışındaki bilgi ve alanlara erişim girişiminde bulunmayacaklarını taahhüt etmişlerdir. Bu nedenle, yetkili olunmayan sunuculara erişilmesi; iç ve dış ağ güvenliğini veya ağ trafiğini bozacak eylemlere girişilmesi yasaktır.
- Şirkete, müşterilere, hizmet verilen diğer üçüncü taraflara ait olan her türlü bilginin açıklanması, çoğaltılması, değiştirilmesi, saptırılması, yok edilmesi, kaybedilmesi, amacı dışında kullanılması, çalınması veya yetkisiz olarak erişilmesi yasaktır.

3. INTERNET KULLANIM KURALLARI

- Şirketin internet kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulur.
- Şirketin internet kaynakları öncelikli olarak Şirket işlerinin gerçekleştirilmesi için kullanılır. Şirket çıkarlarıyla çakışmayacak, Şirket’e zarar vermeyecek veya itibarını sarsmayacak şekilde internet kaynaklarının kişisel kullanımına izin verilmektedir.
- İnternet’ten temin edilecek ve iş için kullanılacak her bilginin güvenilirliğinden şüphe duyulmalı ve alınan bilginin eski ve hatalı olma olasılığı olduğu bilinmelidir.
- Kullanıcılar kişisel bilgisayarları ve/veya mobil cihazları üzerinden kendi kullanıcı hesaplarıyla internet üzerinde gerçekleştirilen tüm işlemlerden sorumludur. Bu nedenle kullanıcılar kullanıcı hesaplarını ve parolalarını uygun şekilde saklar ve başkaları ile paylaşamaz ve “**Şifre Talimatı**”’na uygun olarak değiştirir.
- İnternetten korsan yazılım, uygunsuz yazılı ve grafik malzemenin herhangi bir şekilde indirilmesi, kendisine ait olmayan parola, kendisine ait olmayan kredi kartı numaraları ile alışveriş yapılması kesinlikle yasaktır. Ayrıca, anti virus programları, kırık programlar, ekran koruyucu, yamalar, masaüstü resimleri, yardımcı, tamir edici programlar gibi her türlü dosya ve programların indirilmesi ve/veya kurulması Bilgisayar İşletim Sistemleri’ne zarar verdiği için yasaktır.
- Şirket malı sayılan, Şirket iç kullanımı için hazırlanmış, Şirket’in müşterileri ile ilişkilerini veya Şirket imajını etkileyecek, Şirket tarafından onaylanmamış, her türlü bilgi, belge, dosya, duyuru ve/veya yazılımın (iş potansiyelleri, birim maliyetleri, fiyatlar, yatırımlar, ihale bilgileri vb.), Şirket tarafından verilen görevler dışında kullanımı ve dağıtılması, internet üzerinden satılması, açıklanması, kiralanması ve/veya başkaca bir yöntem ile Şirket dışındaki üçüncü kişilere herhangi bir nedenle iletilmesi kesinlikle yasaktır. Şirket’e ait önemli bilgilerin yetkisiz kişilere verildiği veya açıklandığı belirlendiğinde veya bu konuda şüphe oluştuğu durumda, **İnsan Kaynakları Yönetmeliği** ve **Disiplin Süreci** uygulanır.

- Şirket kaynakları, uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz.

4. YAZILIM KULLANIM VE FİKRİ MÜLKİYET HAKLARINA UYUM KURALLARI

Şirket bilgisayarlarına kurulan yazılımlar **"Şirket Varlık Yönetimi Süreci"** uyarınca yönetilirler.

- Şirkete ait yazılımlar kullanılırken ilgili yasa ve düzenlemelere uyulacaktır.
- Yazılımlar ilgili lisans, uyarı, kontrat ve anlaşmalar uyarınca kullanılacaktır.
- Şirket için veya Şirket adına kullanım hakkı alınmış olan, Şirket çalışanları veya Şirket için geliştirilmiş olan tüm yazılımlar Şirket varlık envanterine kayıtlı olup Şirket malıdır.
- Kullanım haklarının ihlalinin önlenmesi için yazılımlar Şirket tarafından güvenilir kaynaklardan ve Satınalma Süreçlerine uygun olarak sağlanacaktır.
- Şirketin internet kaynakları ve haberleşme alt yapısı, onaylanmamış, ücretsiz ticari hiçbir yazılım için kullanılamaz. Şirket izni olmadan ticari hiçbir yazılım kopyalanamaz, gönderilemez, alınamaz veya çoğaltılamaz.
- Yazılım ve diğer ürünler için, yalnız lisanslı sürümlerin lisans adetleri dahilinde kullanıldığı, Şirket tarafından yapılacak kontrollerle denetlenecektir.
- Lisans veya sözleşmelerinde aksi belirtilmediği sürece yazılımların, yedekleme ve arşivleme dışında, herhangi bir şekilde kopyalanması ilgili Mevzuata göre suçtur. Kanunlarca yasaklanmasının yanı sıra, izinsiz yazılım kopyalanması işbu Politikanın ihlal edilmesi anlamına gelmektedir.

5. ANTİ-VİRÜS POLİTİKASI

- Şirket bilgisayarlarında lisanslı anti-virüs yazılımı yüklenir ve daimi çalışmaları sağlanır.
- Anti-virüs yazılımı yüklü olmayan bilgisayarların, kullanıma açılması ve Şirket ağına bağlanmaları yasaktır. Anti virüs yazılımı yüklü olmayan bilgisayarlar tespit edildiğinde, Şirket'in ilgili birimine haber verilecektir.
- Hiçbir kullanıcı anti-virüs yazılımını kullandığı sistemden kaldıramaz ve başka anti-virüs yazılımını sistemine kuramaz.
- Zararlı virüs programlarını (örneğin; virüsler, solucanlar, truva atı, e-posta bombaları vb.) Şirket bünyesinde oluşturmak ve dağıtmak yasaktır.
- Anti virüs yazılımı kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, vs) özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.

6. ELEKTRONİK POSTA KULLANIM KURALLARI

- **Şirket e-posta kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulur.**
- **Şirket e-posta kaynakları öncelikli olarak resmi ve onaylı Şirket işlerinin gerçekleştirilmesi için kullanılacaktır.**

1. Şirket çalışanları tanımlanan görevlerinin yerine getirilmesinde kendilerine sağlanacak şirket kaynaklarını kullanarak elektronik posta gönderecek / alacaklardır.

2. Şirket çalışanları kendi kullanıcı hesaplarıyla gerçekleştirilen tüm e-posta işlemlerinden sorumludur.
3. Şirket çalışanları kendi yetki alanlarındaki kurumsal elektronik postaların yetkisiz kişiler tarafından görünmesi ve okunmasını engellemekten sorumludurlar.
4. E-posta sistemlerinde parola kullanılır. Kişisel parolalar, Şirketin yetkili sorumluları dahil üçüncü kişilere gösterilemez veya başkalarıyla paylaşılamaz. Aksi durumlarda, parolasını paylaşan kişi parolayı öğrenen kişinin kendisi adına yapacaklarının sorumluluğunu kabul etmiş sayılır. Kişisel parolalar, çalışanın iş sözleşmesinin sonlandırılması ve acil durumlarda Admin Yetkili Sorumlu tarafından iptal edilir.
5. Elektronik posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunur.

- **Şirket çalışanları elektronik postalarını düzenli olarak kontrol etmelidir.**
  1. E-postalar mümkün olan en kısa sürede yanıtlanacak veya ilgili kişiye yönlendirilecektir.
  2. E-posta eklentileri kritik ve değerli olan dokümanlar **"Sunucu Güvenlik Talimatı"** 'na uygun şekilde arşivlenecektir.
  3. "Konu" kısmında "Duyuru" yazmasa bile "Kime" kısmında çok kullanıcıyı içeren **Duyuru amaçlı e-postaların gönderilme yetkisi İnsan Kaynakları Departmanı'ndadır.** Duyuru amacıyla gönderilecek olan e-postalar İnsan Kaynakları Müdürü'nün kontrolünden sonra, İnsan Kaynakları Müdürü tarafından ilgililere duyurulur.
  4. Şirket dışına gönderilen tüm e-postalarda aşağıdaki uyarı mesajı bulunacaktır:

"*Bu e-posta mesajı ve ekleri gönderildiği kişi ya da kuruma özeldir ve gizlidir. Ayrıca hukuken de gizli olabilir. Hiçbir şekilde üçüncü kişilere açıklanamaz ve yayınlanamaz. Eğer mesajın gönderildiği alıcı değilseniz bu elektronik postanın içeriğini açıklamanız, kopyalamanız, yönlendirmeniz ve kullanmanız kesinlikle yasaktır ve bu elektronik postayı ve eklerini derhal silmeniz gerekmektedir. ONCOSEM A.Ş. bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda herhangi bir garanti vermemektedir. Bu nedenle bu bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından, saklanmasından ve kullanılmasından sorumlu değildir. Bu mesajdaki görüşler gönderen kişiye ait olup, ONCOSEM A.Ş.'in görüşlerini yansıtmayabilir*.

This e-mail and its attachments are private and confidential and intended for the exclusive use of the individual or entity to whom it is addressed. It may also be legally confidential. Any disclosure, distribution or other dissemination of this message to any third party is strictly prohibited. If you are not the intended recipient you are hereby notified that any dissemination, forwarding, copying or use of any of the information is strictly prohibited, and the e-mail should immediately be deleted. ONCOSEM A.Ş. makes no warranty as to the accuracy or completeness of any information contained in this message and hereby excludes

any liability of any kind for the information contained therein or for the transmission, reception, storage or use of such information in any way whatsoever. The opinions expressed in this message are those of the sender and may not necessarily reflect the opinions of ONCOSEM A.Ş.. "

- **Şirket çalışanlarının elektronik posta kullanımında ahlaki kurallara ve yürürlükteki mevzuata uygun hareket etmeleri zorunludur.**
    1. Şirket çıkarlarıyla çatışmadığı sürece ve sistemi gereksiz meşgul edecek büyüklükte olmamasına dikkat etmek şartı ile e-posta kaynaklarının kişisel kullanımına izin verilmektedir.
    2. Çalışanlar, elektronik posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.
    3. Kişisel kullanım için İnternet'teki listelere üye olunması durumunda Şirket elektronik posta adresleri kullanılmaz.
    4. Şirket elektronik posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
    5. Şirketin e-posta sistemi ücretsiz veya ticari hiçbir yazılımın alınması, Bilgi işlem bölümü bilgisi haricinde gönderilmesi veya saklanması için kullanılamaz.
    6. Kullanıcıların bilgi paylaşımını elektronik posta yönlendirme, dosya sunucuları ve diğer yetkilendirilebilir Bilgi Güvenliğinin belirlemiş olduğu mekanizmalarını kullanarak yapmaları gerekir.
    7. Şirket çalışanları dışında sistem üzerinde elektronik posta kutusu yaratılmaz.

- **Kullanıcılar gereksiz elektronik postaları silmekle yükümlüdür.**
    1. Elektronik postalar virüs, elektronik posta bombaları ve Truva atı gibi zararlı kodlar içerebilirler.
    2. Kaynağı bilinmeyen elektronik postalar ve ekinde gelen dosyalar; zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren elektronik postalar; kullanıcı kodu/parolasını girmesini isteyen elektronik postalar herhangi bir işlem yapılmaksızın Bilgi İşlem Departmanı'na bilgi verilecek; kesinlikle açılmayacak, yanıt yazılmayacak ve derhal silinecektir ve kesinlikle başkalarına iletilmeyecektir.

- **E-posta Yazılımı**
    1. Kullanıcılar sadece Şirketin yetkili birimlerince onaylanmış e-posta yazılımlarını ve konfigürasyonlarını kullanabilirler.
    2. E-posta yazılımının mevcut güvenlik ayarlarını değiştirmek yasaktır.
    3. Kullanıcılar e-posta yazılımında gönderen kimliğini gizleyecek özelliklerini kullanmaları yasaktır.

- **Şirket kullanıcıları için elektronik posta hesabı alımı ve kullanımı, kullanımdan kaldırılması, İnsan Kaynakları departmanı bilgilendirilmesi ile Bilgi Teknolojileri Yöneticisi tarafından yönetilir.**
- **Tüm elektronik posta sistemleri ve bu sistemler üzerinde yaratılan, tutulan ve/veya saklanan mesaj, bilgi ve dosyaların hepsi (yedeklenen kopyaları dahil) Şirket bilgi varlığı olarak kabul edilmektedir.**
- **Güvenliğinden emin olunmayan bilgisayarlardan (örneğin internet cafe gibi ortak kullanım alanındaki bilgisayarlar) web e-posta sistemi kullanılamaz.**

7. İZLEME VE DENETLEME HAKLARI

Şirket aşağıdaki haklarını saklı tutar; ve çalışanlar Şirket'in izleme ve denetleme haklarını işbu Politikayı okuyarak haberdar olmuş ve kabul etmişlerdir.

- Bilgi güvenliği yönetim sistemleri ve bu sistemlerle gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak denetleme,
- İnternet sistemleri kullanılarak yapılan tüm işlemleri izleme,
- Şirket, e-posta sistemleri kullanılarak yapılan tüm işlemleri izleme,
- Tespit edilen ve lisans anlaşmalarına uymayan yazılımları kullanıcıya haber vermeden kaldırma,
- Kullanıcının yazılımlarla gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını,
- Kullanıcının internet sisteminde, e-posta sisteminde, ortak kullanım sunucularında ve taşınmaz veya taşınabilir şirket mobil araç ve ekipmanlarında gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma

8. UYGULAMA VE CEZA

Bilgi Güvenliği Politikası'na ve burada belirtilen diğer politika, süreç ve talimatlara uymayanlar hakkında **Disiplin Süreci** başlatılacak olup; soruşturma neticesinde uyarma, kınama, para cezası, sözleşme feshi yollarından bir ya da birden fazlası uygulanacaktır.

Gerekli görüldüğü durumlarda yasal işlem başlatılacaktır.