



BİLGİ GÜVENLİĞİ POLİTİKASI

KVKK_P5 VERSİYON 1.00

ELOPSİS ELEKTRONİK OPTRONİK SAVUNMA SİSTEMLERİ A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç:

Bilgi, Elopsis Elektronik Optronik Savunma Sistemleri 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 ulaşılmaya 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 Elopsis Elektronik Optronik Savunma Sistemleri 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 varlıklarının korunması, Elopsis Elektronik Optronik Savunma Sistemleri 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 Elopsis Elektronik Optronik Savunma Sistemleri 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. TÖGEK'in ilgili kısımlarında gizlilik derecesi Gizli ve daha yüksek olan 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 TÖGEK kapsamında belirlenen en 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 kullanımını 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 kullanıcılarıdır. 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 Bilgi Sistemleri Sorumlusuna durum raporlanmalıdır. İlgili kişiler Bilgi Sistemleri Sorumlusu ya da Güvenlik Koordinatörü ile bu amaçla doğrudan iletişime geçebilirler. (İrtibat bilgileri için bkz. Bölüm 7.1)

3.4. Bilgi Sistemleri Sorumlusu

Bilgi Sistemleri Sorumlusu, bilgi ve iletişim teknolojileri kaynaklarının kontrolü ve günlük bilgi güvenliği faaliyetlerinin gerçekleştirilmesinden sorumludur. Bilgi Sistemleri 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. Elopsis Elektronik Optronik Savunma Sistemleri A.Ş. yürürlükteki tüm Türk kanunları ve idari düzenlemelerine riayet etmekle mükelleftir. Bilgi güvenliği bakımından ise 5651 sayılı İnternet 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, 5202 sayılı Savunma Sanayii Güvenliği Kanunu, MSY 317-2 (C) Milli Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi, 04 Haziran 2010 tarihli Savunma Sanayii Güvenliği Yönetmeliği ve 2007/12937 nolu Sabotajlara Karşı Koruma 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 ve gerekli hallerde adli tahkikat 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. Elopsis Elektronik Optronik Savunma Sistemleri A.Ş. bünyesinde kullanılan veri kaynakları ile ilgili detayların yer aldığı bir Veri Envanteri tutmaktadır. Departman Sorumluları 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 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanununun 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 Tesis Özel Güvenlik El Kitabı ile Şirketin politika ve direktiflerine uygunluğunu temin etmek 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 derhal Bilgi Sistemleri Sorumlusunu 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/Sorumlusuna İrtibat Bilgileri:

ELOPSİS ELEKTRONİK OPTRONİK SAVUNMA SİSTEMLERİ A.Ş.

Telefon: + 90 312 441 07 50

Faks: + 90 312 441 07 52

Elektronik Posta: kvkk@elopsis.net

7.3. Bir veri güvenliğini ilgilendiren olayın gerçekleşmesi ya da gerçekleşmesinden şüphe edildiği durumlarda Bilgi Sistemleri 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 Bilgi Sistemleri Sorumlusu ya da Güvenlik Koordinatöründen görüş alınabilir.

8. VERİ GÜVENLİĞİ EĞİTİMLERİ

8.1. Bilgi Sistemleri 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 Bilgi Sistemleri 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 talimatlarda 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 varlıklarının 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 şart koşulacaktır.

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.

11.IT KAYNAKLARININ KULLANIM KOŞULLARI

Şirketin IT kaynaklarını kullanacak herkes aşağıda açıklanan hususları kabul etmiş sayılır:

- 11.1. IT kaynakları, Şirketin faaliyetlerinin yürütülmesi için tedarik edilen her türlü donanım, yazılım, hizmetler ve kaynakları ifade eder. Tüm bilgisayar ağları, kablolu veya kablosuz bilgisayarlar, yazıcılar, mobil cihazlar, depolama cihazları, görsel-işitsel sistemler ve Bulut hizmetleri IT kaynakları içerisinde değerlendirilir.
- 11.2. Her kullanıcı IT kaynaklarının güvenli kullanımı konusunda kendisine verilen tavsiyeleri anlayarak uygulamalı ve Bilgi Güvenliği farkındalığı eğitimlerine katılmalı ve Bilgi Güvenliği Farkındalık Bildirimi hakkında bilgi sahibi olmalıdır;
- 11.3. Şirketin IT kaynaklarının kullanımı ve bu kaynakların Şirket dışı kaynaklara erişim sağlanması için kullanımı sadece Şirket faaliyetleri için gerekli olan araştırma, öğrenme, idari ve sair izin verilen kullanımlar ile sınırlı olmalıdır. Önceden izin alınmaksızın kişisel ticari çalışmalar için IT kaynaklarının kullanımı yasaktır;
- 11.4. Şirket namına yürütülen faaliyetler sadece Şirket tarafından sağlanan bilgi işlem araçları kullanılarak yerine getirilmelidir. Şirket işlerini yürütmek için Şirket dışı bilgi hizmetlerini kullanmak, Şirket verilerini riske atar ve bu nedenle yeterli gerekçelendirme olmadan kullanılmaları yasaktır. Örneğin, Dropbox ya da One Drive ve Gmail, Hotmail gibi e-mail servisleri yerine Şirket e-mail servisi kullanılmalıdır.
- 11.5. Şirketin IT kaynaklarının bireysel amaçlarla kullanımı kesinlikle yasaktır.
- 11.6. Ağ anahtarları, dağıtıcı, kablosuz erişim noktaları ve yönlendiriciler gibi aktif ağ cihazlarının Şirket ağına bağlanması yasaktır. Tüm IP adresleri yalnızca Şirket tarafından tahsis edilecek ve yönetilecektir;
- 11.7. Çalışanlar önceden yazılı olarak açık bir şekilde izin verilmediği sürece Şirket dışı misafir vb. kişilerin Şirketin bilgi işlem servislerine erişim sağlaması yasaktır;
- 11.8. ELOPSİS ELEKTRONİK OPTRONİK SAVUNMA SİSTEMLERİ AŞ'ye ait IT kaynaklarını kullanan her kullanıcı, IT ve Elektronik Haberleşme Kaynaklarının Kabul Edilebilir Kullanım Politikası ve ilgili tüm yasal ve diğer hükümler, düzenlemeler, kurallar ve uygulama kuralları dâhil olmak üzere Şirket Bilgi Güvenliği Politikasına ve Tesis Özel Güvenlik El Kitabına uygun hareket etmekle mükelleftir. Özellikle, ancak bunlarla sınırlı kalmamak koşuluyla, her kullanıcı aşağıda yer alan bentlerde belirtildiği gibi hareket etmekle mükelleftir:
 - 11.8.1. Şirket tarafından kendisine tahsis edilen şifre ve kullanıcı adını kimseye ifşa edilmeyecek ve Şifre ve Kullanıcı Adları hakkında Uygulama Esaslarına uygun hareket edilecektir;
 - 11.8.2. Şirket nezdinde ya da haricinde izin verilen amaçlar haricinde IT kaynaklarına erişilmeyecek ya da diğer kişilerin izin verilmeyen amaçlarla bu kaynaklara ulaşmasına aracılık edilmeyecektir;
 - 11.8.3. Şirket içerisinde ya da başka bir yerde herhangi bir IT kaynağına port taraması gibi izinsiz erişim, değişiklik, arızalandırma eylemleri gerçekleştirecek materyal ya da kaynaklar kullanılamaz ve ağına sokulamaz;

- 11.8.4. Saldırgan olarak değerlendirilebilecek veya Şirketin kurumsal itibarını zedeleyebilecek pornografik, pedofilik, cinsiyetçi, ırkçı, iftira niteliğinde, tehdit edici, karalayıcı, yasa dışı, ayrımcı veya terörist nitelikte görüntülü ya da sesli materyal içeren resimler veya metinler sergilenemez, sistem ve dosyalarda saklamaz, alınamaz veya iletmez;
- 11.8.5. Elektronik posta imzaları ve / veya başlıkları taklit edilemez, "zincirleme", "gereksiz" veya "taciz edici" e-postalar düzenlenemez ve / veya iletilemez, elektronik iletişimde başkalarının kimliğine bürünmek suretiyle başkaları adına işlem yapılamaz ve gereksiz veya saldırgan iletişimler oluşturmaz;
- 11.8.6. Şirketin IT hizmetleri kapsamında sunduğu kaynaklara erişim için kullanılan tüm mobil cihazlar uygun şifreleme yazılımları kullanılarak şifrelenmiş ve pin kodu veya şifre ile korunur olması sağlanacaktır;
- 11.8.7. Şirket ve üçüncü şahıslar tarafından sağlanan tüm materyallerin ve yazılımların telif hakkına saygı gösterilecek ve yazılım ve alınan veriler dâhil olmak üzere telif hakkı kapsamındaki materyaller telif hakkı sahibinin izni veya Şirket tarafından sahip olunan lisan koşulları haricinde kullanılmayacak, indirilmeyecek, kopyalanmayacak, sistemde bulundurulmayacak veya tedarik edilmeyecektir;
- 11.8.8. Gerçek kişiler hakkındaki veriler işlenirken veri koruma mevzuatı hükümlerine uygun olarak işlemek (yani toplamak, kullanmak, paylaşmak ve imha etmek) için Şirketin Veri Koruma Politikasına uygun hareket edilecektir.
- 11.8.9. Şirket IT kaynakları üzerinde kullanıcılar tarafından oluşturulan / sahip olunan / depolanan tüm bilgi varlıklarının, yasaklanan fiillerin işlenmesinden şüphelenilmesi durumunda, Şirket veya yasal yetkililer tarafından denetime tabi tutulabileceği unutulmamalıdır. İlgili verilerin şifrelenmesi durumunda, kullanıcının şifre çözme anahtarını sağlaması zorunludur;
- 11.8.10. Herhangi bir platform aracılığıyla kullanılan her türlü materyal ve yazılım için lisans koşullarının ne olduğunu belirlenerek ilgili koşullara uygun hareket edilmelidir;
- 11.9. 5561 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun Erişim sağlayıcının yükümlülükleri başlıklı 6. Maddesi ve Tesis Özel Güvenlik El Kitabı 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 tedbirlerin uygulama usulleri Elektronik Haberleşme ve Verilerin Denetlenmesi Hakkında Uygulama Esasları ile düzenlenecektir.
- 11.10. Veri güvenliğini ilgilendiren bir olayın gerçekleşmesi ya da gerçekleşmesinden şüphe edildiği durumlarda Bilgi Sistemleri 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.
- 11.11. Daha fazla incelemenin gerekli olması durumunda, Bilgi Sistemleri Sorumlusu, Şirket Yönetim Kurulunun açık izni ile Şirket ağındaki herhangi bir sistemi incelemek için gerekli tedbirleri alabilir.
- 11.12. Yürürlükteki yasal zorunluluklar haricinde, Şirket, kendisi tarafından sağlanan ve / veya yönetilen herhangi bir IT kaynağının doğrudan veya dolaylı olarak

kullanımından veya kullanımının önlenmesinden kaynaklanan herhangi bir kayıp, hasar veya olumsuzluktan sorumlu tutulamaz.

- 11.13. Her ne kadar Şirket, kişisel ve diğer verilere yetkisiz erişim, değişiklik yapılması, verilerin ifşa edilmesi, imha veya kaza sonucu kayıplara karşı uygun güvenlik önlemlerini almakta ise de, kullanıcıya verilerin güvenliği, gizliliği veya bütünlüğü hakkında hiçbir garanti veya taahhütte bulunmaz.
- 11.14. Kullanıcıların adı, adresi, fotoğrafı, medeni durumu, e-posta adresi, oturum açma adı, takma adı, Şirket kimlik kartı ve diğer ilgili bilgiler, yönetim ve sistem kullanımının denetlenmesi gibi diğer amaçlarla kullanılmak üzere bilgisayar teknolojileri ile işlenmiş ve uygun koruma sağlanan ortamlarda saklanacaktır.
- 11.15. Yukarıda zikredilen koşullar Şirkete ait olmayan kişisel dizüstü bilgisayarlar, ev bilgisayarları gibi cihazların Şirket ağını kullandığı süre boyunca doğrudan ve / veya VPN aracılığıyla Şirket ağına bağlandıkları kullanımlar için de geçerli olacaktır.
- 11.16. Yukarıda zikredilen koşulların ihlali, tüm Şirket IT kaynaklarının kullanma yetkisinin belirli süreler için askıya alınmasını ve / veya ceza verilmesi ile sonuçlanabilecek disiplin soruşturması açılmasına neden olabilir. Ağır ihlal durumlarında Şirket ilgili ile akdedilen iş sözleşmesinin feshi ve ilgili kullanıcı aleyhinde hukuk ve ceza davaları açma hakkını saklı tutar.
- 11.17. Şirketin IT imkânlarını kullanan ve/veya Şirket tarafından sağlanan internet bağlantısı kullanan misafirler için Şirket çalışanları vekil olacaktır. Vekil olarak hareket eden çalışanlar misafirlerinin eylemlerini tespit etmeli ve sorumluluğunu almalıdır. Ziyaretçilerin kontrollü bölge ve oda ile kırmızı mimari alan gibi erişim yetkisi sınırlandırılmış korumalı alanlara erişimine müsaade edilmeyecektir. Bahse konu alanlara ziyaretçi girişlerinin ne şekilde olacağı Tesis Özel Güvenlik El Kitabı BÖLÜM 11'de açıklanmıştır.