İNTERNET VE ELEKTRONİK İLETİŞİM ARAÇLARININ KABUL EDİLEBİLİR KULLANIMI HAKKINDA USUL VE ESASLARA İLİŞKİN POLİTİKA

KVKK_P9 VERSİYON 1.00

ELOPSİS ELEKTRONİK OPTRONİK SAVUNMA SİSTEMLERİ A.Ş.

İNTERNET VE ELEKTRONİK İLETİŞİM ARAÇLARININ KABUL EDİLEBİLİR KULLANIMI HAKKINDA USUL VE ESASLARA İLİŞKİN POLİTİKA

1. GİRİŞ

Elopsis Elektronik Optronik Savunma Sistemleri A.Ş. özel hukuk tüzel kişisi sıfatıyla şirket nezdinde tahsis edilen tüm şirket kaynaklarının amacına uygun kullanımını sağlamak ve kötü amaçla ya da kullanım amacıyla uyuşmayan uygunsuz biçimlerde kullanılmasını önlemekle mükelleftir. Bu sorumluluk elektronik posta (e-mail) ve internet erişimi gibi kullanımları da içerisine almaktadır.

2. AMAÇ VE KAPSAM

İşbu politikanın amacı Şirketimiz nezdinde istihdam edilen çalışanların internet, e-mail vb. elektronik iletişim amaçlarını kullanırken gözetmesi gereken usul ve esasları belirlemektir. İşbu Politika hükümleri hiçbir şekilde üzerinde gizlilik dereceli bilgi barındırmayan, piyasa araştırması, ihale ilanları takibi, teklif verme, teklif dosyası hazırlama gibi faaliyetler için internet aracılığıyla dış ortama açık, kırmızı yapılanma dışında kalan diğer sistemler için geçerli olup kontrollü bölge ve odalar gibi gizlilik dereceli bilgilerin işlendiği, alınıp gönderildiği, sadece yetkili kişilerin üzerinde işlem yapabildiği, dış erişime kapalı birimlerle ilgili olarak Tesis Özel Güvenlik El Kitabının ilgili hükümleri uygulanır.

İşbu Politika üç kısımdan oluşmaktadır:

- İnternet Kullanım Politikası
- E-mail Kullanım Politikası
- Çalışanlar arasında elektronik iletişimler

İşbu Politika aşağıda sıralanan politika belgeleriyle birlikte değerlendirilmelidir:

- Şirket Disiplin Tüzüğü
- Veri Koruma ve İşleme Politikası
- Bilgi Güvenliği Politikası

İşbu Politika açısından e-mail, web mail, anlık mesaj ve web forumları da dâhil olmak üzere tüm elektronik iletişim biçimlerini ihtiva edecek şekilde yorumlanmalıdır. Şirket tarafından sağlanan internet ve e-mail imkânlarının Şirket binası içerisinde kablosuz ağa bağlanarak ya da dışarıdan masaüstü erişim yoluyla kullanıldığı takdirde işbu Talimatname hükümlerinin ilgili tarafından kabul edildiği varsayılacaktır.

3. İNTERNET KULLANIM POLİTİKASI

3.1. Hizmet Sunumunun Amaçları ve Kullanıcıların Sorumlulukları:

İnternet hizmeti münhasıran Şirketin iş faaliyetleri için tedarik edilmektedir. Özellikle internete çalışanların şahsi işleri ve haberleşmeleri için kullanılamaz.

3.2.Kullanımın Takibi:

3.2.1. Şirket bünyesinde kurulu internet ağını kullanan çalışanlar açısından makul bir özel hayatın gizliliği ya da mahremiyet beklentisi söz konusu değildir. Şirket internet aramalarının kaydedilmesi ve çalışanların kullanımı için uygun olmayan site ve bağlantılara (link) erişimin engellenmesi için **GÜVENLİ AĞ HİZMETLERİ** kullanmaktadır. Bahse konu sistem Bilgi Sistemleri Sorumlusu tarafından yönetilmekte olup Departman Sorumluları ve Yönetim Kurulu tarafından takip edilmektedir. Sistemin olası eksiklik ya da boşluklarını tespit etme için firewall aralıklarla sınanmaktadır.

3.2.2. Gözetim yazılımı Şirket internet ağının kullanımını gözlemlemekte ve Bilgi Sistemleri Sorumlusu ile Departman Sorumluları, Şirket politikalarına uygun bir şekilde kullanım sağlanmasını temin etmek için tutulan ağ log kayıtlarını gözlemlemekte ve denetlemektedir. Bu kapsamda bilgisayarların monitörleri uzaktan taranmakta, dosyalar ve e-mailler çek edilmekte ve ziyaret edilen internet siteleri analiz edilmektedir. Yazılım, ilgili kullanıcı ismi ve ziyaret gün/saat detayları ile birlikte ziyaret edilen tüm web sitelerini kaydetmekte olup gözetim amacıyla düzenli raporlar hazırlamaktadır. Kötüye kullanım ya da şüpheli içerikli ziyaretler ve siteler otomatik olarak raporlanarak olağan disiplin prosedürleri işletilecektir. Şirket internet ağına erişim sağlamak suretiyle, kullanıcılar yukarıda açıklanan gözetim ve internet erişiminin denetlenmesi faaliyetlerine rıza göstermiş sayılırlar.

3.3.Kişisel Abonelik ve Dinlenme Amaçlı Kullanım:

Çalışanlar, Bilgi Sistemleri Sorumlusu ile yazılı olarak kararlaştırılmadıkça, Şirket nezdinde internet servis sağlayıcılarına ve / veya çevrimiçi hizmetlere özel abonelikler alamaz ve bunları Şirketin bilgisayar ekipmanında kullanamaz. Çalışanlar İnternet hizmetini bilgisayar oyunu veya kumar gibi uygun olmayan eğlence amaçları için kullanamazlar.

3.4.Şirketin itibarına Zarar Verecek Eylemler:

Çalışanlar, interneti Şirketin çıkarlarına aykırı olarak ya da Şirket ve ortaklarını zor durumda bırakacak ve kurumsal itibarına zarar verecek bir biçimde kullanamazlar. Örneğin, yasaklanmış ya da kanuna aykırı materyal içeren web sitelerine abonelik ya da telif hakkı sahibinin açık izni olmaksızın üçüncü tarafların telif hakkı ile korunan içeriklerini kullanmak ya da indirmek.

3.5. Yazılım Yüklemek(Downloading):

Virüs risklerini minimize etmek ve ağın içerisinde lisanssız yazılım bulunmasını önlemek amacıyla Şirket ağı kullanılarak yazılım yüklenmesi yasaktır. Söz konusu yasak oyun ve ekran koruyucusu yazılımları için de geçerlidir. Personelin eğitilmesi amacıyla bahse konu yasağa istisna getirilmesi gerekiyorsa lütfen Bilgi Sistemleri Sorumlusu ile irtibata geçiniz.

3.6. Yasadışı Kullanım:

Çalışanlar bilinçli bir şekilde interneti T.C. kanunlarına aykırı olan faaliyetler için kullanamazlar. Çalışanlarımız, cinsiyet, ırk, dini inanç, cinsel eğilim, engellilik veya başka nedenlerle diğer çalışanları incitecek ya da ayrımcılığa maruz kalmalarını sağlayacak nitelikteki materyalleri bulmak, indirmek, erişmek veya başka bir şekilde araştırmak için İnternet servisini kullanamaz.

3.7.Çevrimiçi Alışveriş:

Çalışanların uzun süre mesaide bulundukları zamanlarda çevrimiçi alışveriş yapmalarına izin verilebilir. Ancak satıcının yazılımlarını bilgisayar ve diğer cihazlarınıza yüklememeniz gerektiği unutulmamalıdır. Her ne kadar sağlanan ağ, bireysel ikamet için kullanılan ağlardaki güvenlikten daha az seviyede güvenlik standartları içermese de Şirketimiz finansal işlemlerin güvenliğinden dolayı sorumlu tutulamaz. Alışverişler kesinlikle "müstehcen, pornografik ya da özel yaşam alanına giren" öğeler içerenler başta gelmek üzere yasaklanmış faaliyetler kısmında belirtilen kategorileri içeremez.

3.8.Güvenlik:

Ağ alanına erişim ve güvenliğinden çalışanlarımız olarak sorumlu olmanız nedeniyle kimseyle kullanıcı ismi ve şifrenizi paylaşmamanız zaruridir. Bu bağlamda Ctrl-Alt-L ya da Ctrl-Alt-Del tuşlarına basılmak suretiyle bilgisayar başında olamadığınız zamanlarda bilgisayarlar kilitli tutulmalıdır. Şirketin e-mail ya da verilerine erişmek için kullanılan bireysel cihazlar kaybolduğunda ya da çalındığında durum derhal Bilgi Sistemleri Sorumlusuna bildirilmelidir. Çalışanlarımız ayrıca şifre koruması ve güvenlik alanlarında ayrıntılı bilgiler içeren Bilgi Güvenliği Politikası hükümleri hakkında bilgi sahibi olmalıdır.

3.9.Yasaklanmış Faaliyetler:

İnternet ortamında yasaklanmış faaliyetler araçların aşağıda sıralanan faaliyetlerin izlenmesi, depolanması dağıtımı ya da başka bir biçimde kullanılmasını içermektedir:

- Yasadışı faaliyetler (telif haklarının her türlü ihlali dâhil olmak üzere)
- Tehdit edici, istismar edici, rahatsız edici ya da ayrımcılık içeren davranış biçimleri
- İftira ve karalayıcı amaçlar ve faaliyetler
- Müstehcen, davetkâr ya da özel yaşamla ilintili mesajlar ya da rahatsız edici imajlar ya da pornografik materyaller
- Önceden izin alınmadığı takdirde Şirketimizin zarara uğramasına neden olabilecek faaliyetler
- E-mail aracılığıyla gönderilen zincirleme mektuplar

- Kar etmek amacıyla yürütülen bireysel ya da ticari faaliyetler
- Kötü niyetli zarar verici eylemler
- Uygunsuz siyasi, dini ya da eğlence amaçlı kullanımlar.

3.10. Koruma Yükümlülüğü:

Şirket ağını kullanırken kazara çocukların istismar edildiği görüntüleri içeren görsellere maruz kalan her çalışan, bahse konu görüntülerin konumunu derhal Bilgi Sistemleri Sorumlusuna bildirmeli ve bu görüntülerin kopyasını almamalı ya da kimseye dağıtımını yapmamalıdır.

3.11. Güvenlik ve Erişim Hususları:

3.11.1. Şirket kendisini ve bilgisayar sistemlerini, web sitelerini ve çalışanlarını gerek ya da muhtemel harici ve dâhili güvenlik tehditlerine karşı korumak için önlemler almıştır. Bu kapsamda alınan güvenlik tedbirleri aşağıdaki unsurları içermekle birlikte bunlarla sınırlı değildir: güvenlik duvarı(firewall) ve gelen/giden internet trafiğini bloke etmek için kullanılan proxy sunucuları, anti-virüs yazılımları, erişim kontrol yazılımı (spesifik web sitelerine erişimi engelleyen), yazılım yüklenmesini önleyen tedbirler, zararlı olabilecek komut dosyası ve unsurlarını kısıtlayan yazılımlar.

3.11.2. Şirket internet sunucusundan filtreleme hizmeti almaktadır. İnternete erişim Şirket tarafından ağını kullanan çalışanları için ek olarak engellenmemekle birlikte, yasa dışı, pornografik ya da diğer rahatsız edici içerikler (örneğin cinsel içerikli mesajlar, web temelli sohbet, suç teşkil eden faaliyetler, uyuşturucu, alkol ve sigara, kumar ve oyunlar, bireysel ve arkadaş bulma siteleri, Usenet haberleri, şiddet ve silah vb.) barındıran ya da barındırdığından şüphe edilen sitelere erişimi engelleyebilir.

3.11.3. İnternet kullanıcıları pek çok web sitesinin bazen gizlice site kullanım detaylarını kaydettiğini ve internete erişim ile faaliyetlerin PC bilgisayar içerisinde faaliyet kaydı bıraktığının bilincinde olmalıdırlar.

3.11.4. Şirket, acilen eylemde bulunulmasını gerektiren bir güvenlik ihlali şüphesi ile karşı karşıya kaldığında ya da Şirketin ağ ve/veya bilgisayar sistemlerinin risk altında olduğunu değerlendirdiğinde önceden haber vermeksizin internet erişimini kesme hakkını saklı tutar.

4. E-MAİL POLİTİKASI VE KILAVUZ İLKELER

4.1. Bu Politikanın amacı e-mail sistemlerinin uygun bir şekilde kullanımını sağlamaktır. E-mail servisine erişim yetkisine sahip olan her bir çalışan işbu Politika hükümlerine riayet etmekle ve e-mail sisteminin sorumluluk bilinci içerisinde etkin ve yalnızca onaylanmış amaçlar için kullanılmasını temin etmekle mükelleftir. Bu politikanın amacı, çalışanların özellikle şirket içi iletişimi için e-mail vasıtasıyla kurulan

iletişimleri için kılavuz işlevi görecek bilgiler vermektir. Örneğin, Şirket e-mail sisteminin kişisel kullanımı yasaktır.

4.2. ELOPSİS A.Ş. Firmasına ait Gizlilik Dereceli Bilgiler (GDB) e-mail yolu ile asla gönderilmeyecek, başka birinden bir GDB e-mail yolu ile alındığı takdirde durum derhal sıralı amirlere bildirilecektir.,

4.3. E-mail İletişimlerinin Statüsü:

Çalışanlarımız, elektronik posta üzerinden iletişim kurarken, e-mail yazışmalarının yasal işlemlerde ifşa edilebilecek bir belge olduğunu her zaman akılda tutmalıdır. Şirketimizin e-mail ağında gönderilen veya alınan tüm e-posta mesajları Şirketin mülkiyetindedir ve kullanıcılar e-posta sistemini kullanırken kişisel gizlilik beklentisi içerisinde olmamalıdır. Bilgi Sistemleri Sorumlusu, şirket politikalarına uyumu sağlamak için e-posta mesajlarını ve ağ günlüklerini izleme yetkisine sahiptir. Tüm kullanıcılar, e-postaların bu şekilde izlenmesini ve incelenmesine rıza göstermiş sayılırlar.

4.4. Kişisel E-mailler:

E-posta sistemi kullanıcıları dâhili ve harici kişisel mesajlar gönderip alabilirler. Fakat bu şekilde kullanımlar, kullanıcının işini yürütmesine veya başka bir kullanıcının çalışmasına engel teşkil etmemeli veya kullanıcının görev ve sorumluluklarına zarar vermemelidir. Kişisel konular için e-posta kullanımı aşırı düzeyde olmamalıdır. E-posta sistemi özel ticari faaliyetler için veya Şirkete ait gizli bilgileri ifşa etmek, dağıtmak veya başka şekilde yaymak için kullanılamaz.

4.5. İçerik:

Tüm e-postaların içeriği, ister açık ister kapalı olsun, cinsel, ırksal veya dini referanslar, suç veya taciz içermemeli ve yalnızca işyerinde profesyonel iletişim için kabul edilebilir sözcükler kullanılarak kaleme alınmalıdır.

4.6. Gizlilik:

E-mail mesajlarının gizliliği garanti edilmez. Gönderilen veya alınan herhangi bir mesaja, ister kazara (örneğin, bilgisayar oturumunun açık bırakılması nedeniyle) veya bilinçli olarak (örneğin, bağlantı sorunlarını teşhis etmek için bir e-postanın açılması gerekebilir), gönderildiği kişi dışındaki meslektaşlar tarafından erişilebilir. Bu nedenle mesajlar özel veya gizli olarak kabul edilemez. Kişisel mesajlar, üçüncü şahısların içeriği gözden geçirme olasılığı hatırlanarak yazılmalıdır. Harici e-postalar söz konusu olduğunda ise, doğaları gereği güvenli değillerdir ve bu tür mesajlar, bilgimiz olmadan üçüncü şahıslar tarafından ele geçirilebilir ve okunabilir. Belirli bir gizlilik veya hassasiyete sahip mesajlar, alternatif bir ortamda ve Bilgi Güvenliği ve Veri Aktarım Güvenliği Politikasında belirtilen yöntemler kullanılarak gönderilmelidir.

4.7.Dosya Eklentileri:

Herhangi bir uygunsuz materyalin şirket ağına kopyalanmasını engellemek ve virüs bulaşma riskini azaltmak için, e-posta mesajlarına dosya ekleri (resim, metin veya elektronik tablo içerikleri), yalnızca güvenilir kaynaklardan yani kimliğini bildiğiniz irtibatlarınızdan gelirlerse ve uygunsuz içerikler barındırmıyorlarsa indirilebilir. E-maile eklenmiş çalıştırılabilir program dosyaları açılmamalıdır. Bunun yerine, bu tür mesajlar tavsiye için Bilgi Sistemleri Sorumlusuna iletilmelidir. Yürütülebilir dosyaların uzantıları şunlardır: .EXE, .COM, VBS. SCR, game.exe ve screen.scr.

Açıklama [r1]: Bahse konu uzantılar örnek olarak sunulmuştur. Bilgi Sistemleri Sorumlusu Şirketin kullandığı uzantıları yazabilir

4.8.Zincirleme Mektuplar/Şakalar:

Zincirleme mektuplar ve şaka içerikli yazışmalar şirket çalışanlarının zamanları ve şirket kaynaklarının uygunsuz kullanımı anlamına gelmekte olup kasıtlı olmaksızın muhatabın alınmasına da neden olabilir. Bu türden mesajlar gelen kutusuna geldiğinde diğer kullanıcılara aktarılmamalı ve ağdan silinmelidirler.

4.9.Asılsız Virüs Uyarıları:

Şirket dışı taraflardan gelen ve virüs uyarısı içeren mesajlar diğer kullanıcılara aktarılmamalıdır. Pratikte bu tür mesajların büyük kısmı asılsızdır. Ancak, her koşulda Bilgi Sistemleri Sorumlusuna haber verilerek tavsiyeleri alındıktan sonra Gelen Kutusundan silinmelidirler.

4.10. Şirket İşlemleri İçin Harici E-mail Sistemlerinin Kullanımı:

Şirket iş ve işlemleri ile ilgili tüm e-posta yazışmaları şirketin e-posta ağı kullanılarak gönderilmelidir. Şirket işleri için özel e-posta sistemleri ve hesaplarının (örneğin, AOL, Hotmail, internet hizmet sunucularının sağladığı elektronik posta hizmetleri ve burada zikredilmeyen sair e-mail servisleri) kullanılması yasaktır. Şirket ağına şirket binası dışındayken erişmesi gereken personel, uzaktan çalışma konusunda tavsiye almak için Bilgi Sistemleri Sorumlusu ile iletişime geçmelidir.

4.11. E-mail Gönderimi İçin Geçerli Kılavuz İlkeler:

4.11.1. E-mail Alıcılarının Belirlenmesi:

a) Dikkatli Bir Şekilde Kontrol Ediniz: Hepsini Cevapla ve Cevapla ikonlarının yanlış kullanımı gibi sık karşılaşılan e-mail gönderi hatalarından kaçınmak için e-mail gönderilmeden önce alıcı adresleri iyi bir şekilde kontrol edilmelidir.

b) Birincil Alıcı: E-posta üst bilgisindeki adres kutusuna birincil alıcıyı girmenin yanı sıra, alıcının kim olduğunu ve kimin yanıt vermesinin beklendiğini açıkça belirtmek için iletinin metin başlığı "xxxx'e mesaj" olmalı veya "Sevgili/Sayın xxxx" başlığı olmalıdır. CC'ler daha sonra yalnızca bilgi için kopyalanmalıdır. Mail atarken CC'ye koyacağınız kişi o iş hakkında bilgi vermek istediğiniz, mailin direk olarak muhatabı olmayan kişidir. Mailde bir kişiyi CC'ye koyarsanız, bu durum maili alan herkes tarafından görülebilir. Yani atacağınız mailde birini CC'ye koyduğunuzda, o kişinin bu mail hakkında bilgi sahibi olmasını ön görürsünüz.

c) CC Listeleri: Her kullanıcının bir not veya mektubun muhatap ve kopya listesini dikkatlice değerlendirmesi gerektiği gibi, bir e-postayı adreslerken de aynı özen gösterilmelidir. Özellikle bir E-postada birden fazla CC listesi kullanılmasından kaçınılmalıdır. Bilgiyi kopyalamak veya kopyalanan her bir kişiden girdi talep etmek için gerçek ve etkili bir amaç olup olmadığı dikkatlice analiz edilmelidir. Müşteri gruplarına gönderilen e-postalar için CC listeleri kullanılmamalı; bu tür iletişimler portal aracılığıyla gönderilmelidir. Alıcıların gizliliğine saygı göstermek için "Kime" veya "Bilgi" kutularında e-posta adresi listelerini kullanmamaya özellikle dikkat edilmelidir.

d) BCC Listeleri: “BCC”, Gizli Karbon Kopya olarak adlandırılır. Kapalı Karbon Kopya olarak da bilinir. Bu alana yazılan e-mail adreslerine de gönderilmek istenilen yazılı mail iletilir. Bu alana yazılan e-mail adreslerini “To” ve “CC” alıcıları göremez. Bu alanı sadece gönderici ve bu alanda yazılı e-mail adres sahibi alıcısı görür. Ancak “BCC” alanına yazılan kişiler, “To” ve “CC”deki alıcıların kimler olduğunu görebilir. Üçüncü şahıslara gönderilen e-postalarda BCC'nin kullanımın uygun olacağı durumlar olsa da, meslektaşlar arasındaki iletişiminde paylaşılması gereke bilgilerin bir veya daha fazla taraftan saklanması kötü bir fikir olabilir çünkü e-postalar daha sonra iletilebilir ve gizli tutulması istenen bilgiler bu şekilde ifşa olunabilir. Meslektaşlar arasında güven sorunları, bazılarının özel olduğunu varsaydıkları mesajlar bu şekilde paylaşıldığında ortaya çıkabilir ve bu nedenle meslektaşlar arasında gizli karbon kopya kullanımından genellikle kaçınılmalıdır.

e) Toplu E-mail Mesajları: Tolu e-mail gönderimi yalnızca şirket faaliyetleri için kullanılmalıdır. Hiç bir şekilde bireysel mesajların aktarılmasında kullanılamaz. Bunun yanı sıra üçüncü tarafların mal ve hizmetlerinin tanıtımının yapılması ya da tavsiye edilmesi de uygun değildir.

f) Belge/Elektronik Çizelge Eklentilerinin Gönderilmesi: E-mail, hatırlatıcı not ya da diğer belge eklentilerinin dağıtımı için kullanılabilir. Ancak 10 MB’ı aşan dosya ve eklentiler e-mail üzerinden gönderilmemelidir. Bilgi Sistemleri Sorumlusu, paylaşılan alanlar gibi yöntemlerle büyük çaplı dosyaların gönderilmesi hususunda gerekli tavsiyelerde bulunabilir.

5. KİŞİSEL VERİLERİN KORUNMASI:

Kişisel verileri içeren her türlü iletişim, yürüklükteki veri koruma mevzuatına tabi olacaktır. Şirketimizin Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Bilgi Güvenliği Politikası kişisel verilerin nasıl güvende tutulacağına dair ayrıntılı bilgiler içermekte olup her çalışan tarafından bilgi sahibi olunmalıdır.