

PRESTİJ TÜTÜN SANAYİ VE TİCARET ANONİM ŞİRKETİ BİLGİ GÜVENLİĞİ, KİŞİSEL VERİ GÜVENLİĞİ VE İLETİŞİM TALİMATI

I. KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI İLE BÜTÜNLEŞİK İŞYERİ BİLİŞİM TEKNOLOJİLERİ KULLANIMI

1. AMAÇ

Prestij Tütün Sanayi ve Ticaret Anonim Şirketi Teknoloji Kullanım Politikasının bir parçası olarak İnternet erişimi ve güvenliği konusunda, Şirket networkü üzerinden İnternet erişiminde bulunan tüm kullanıcılar için geçerli olan ortak kural ve koşulları açıklamaktır.

Şirket bu Talimat ile ayrıca 6698 Sayılı Kişisel Verilerin Korunması Kanunu gereğince oluşturduğu muhtelif Politikalar, KVKK Kurulu(Komitesi) ve ilgili görev tanımlarının yanında, tüm çalışanların farkındalıklarının artması, görev ve sorumlulukların açıkça ortaya konulması anlamında Kişisel Verilerin Korunması hakkında da asgari korumayı gerçekleştirmeyi amaçlamaktadır.

2. KAPSAM

Tüm Şirket personeli ve geçici süreli çalışılan danışmanları kapsamaktadır.

3. GENEL AÇIKLAMA

İşyerinin faaliyetleri ile ilgili herhangi bir veri işyerine mahsus bilgi olarak değerlendirilir.

Kişisel Veri ise ilgili mevzuat ve işyerinde oluşturulmuş Politikalar anlamında korunan Kişisel Verileri ifade eder.

İşyeri faaliyetlerinin verimli ve tam zamanında gerçekleştirilebilmesi için, bu bilgi ve veriler mevzuata uygun ve düzenli yönetilmelidir.

İşyerine mahsus bilgi, faaliyet alanları ile ilgili olmadıkları sürece kütüphaneden alınan kitaplar, araştırma ya da ders notlarını kapsamaz. Bu faaliyetlere dahil olanlar (fakat sadece bunlarla sınırlı olmamak şartıyla) finansal, iletişimsel ve fiziksel veri kaynaklarıdır. Bunlara, hangi ortamda saklanırsa saklansın bölüm ve ofis seviyesindeki bütün bilgiler dahildir.

4. BİLGİYE VE KİŞİSEL VERİLERE ULAŞIM

İşyerine mahsus bilgiler, işverenin en değerli varlıklarından biridir ve bu bilgilerin kullanımını dikkat ve özen gerektirir. Çalışanlar, bilginin bütünlüğünü, doğruluğunu ve gizliliğini korumakla yükümlüdür.

Kişisel Veriler ise gerek ilgili mevzuat tarafından sağlanan korunma güvencesi, gerek ise işveren bakımından sahip olduğu önem dolayısıyla yine işverenin en değerli

varlıklarından biridir ve bu bilgilerin kullanımı sorumluluk, dikkat ve özen gerektirir. Çalışanlar, verilerin bütünlüğünü, doğruluğunu ve gizliliğini korumakla yükümlüdür.

Çalışanlar bilgilerin ve kişisel verilerin kullanımında sorumluluklarının farkında olmalı ve sahip oldukları bilgileri yetkisi bulunmayan kişilere aktarmamalı, yetkisi dışında kullanmamalı, gereksiz değişiklikler yapmamalı veya bilgileri yok etmemelidirler.

İşyerine mahsus bilgilere ve kişisel verilere erişim hakkı, ihtiyaçlar dahilinde, iş tanımları çerçevesinde yetki verilmiş çalışanlara ve ilgili üçüncü kişilere verilir. Bu erişim hakkı aktarılamaz, paylaşılamaz ya da başka birine devredilemez. Kurallara uymayanlar için disiplin hükümleri uygulanacaktır.

5. ÇALIŞANLARIN SORUMLULUKLARI

Çalışanlar ve ilgili üçüncü kişiler, işyerine mahsus bilgilerin ve kişisel verilerin güvenliğinden sorumludur. Bu talimatta belirtilen hususlar, yapılması gerekenler için minimum kıstaslar olarak alınmalıdır. Çalışanlar ve ilgili üçüncü kişiler işyerine mahsus bilgilerin ve kişisel verilerin korunması ve güvenliği için uygun gördükleri bütün önlemleri almalıdırlar.

Aşağıdakiler çalışanların ve ilgili üçüncü kişilerin sorumluluklarının ana hatlarını göstermektedir.

- İzinsiz olarak bilgi ve kişisel verilerin erişiminden ve kullanımından sakınılmalıdır.
- Sistem yönetici bilgisayarlarına izinsiz erişim girişiminde bulunan çalışanlara ilgili disiplin hükümleri uygulanır.
- İlgili üçüncü kişilerin, bilgiye ve kişisel verilere hukuka aykırı olarak erişimlerinden dolayı işyerinin bu kişilere başvuru hakları saklıdır.
- Çalışanlar ve ilgili üçüncü kişiler, kendilerine iş amaçlı sağlananlar dışında, diğer bilgisayarlara, amirlerinin/ kendilerini yetkilendirenlerin yazılı izni olmaksızın erişim yapmamalıdır.
- Çalışanlar ve ilgili üçüncü kişiler, işleri için özel olarak kendilerine sağlanan bilgiler ve kişisel veriler dışında, şirket bilgilerini ve kişisel verileri kullanamaz, (bilgiler ve kişisel veriler korumasız bir alanda bulursa dahi) ve yetkili olmadıkları sürece şirket bilgilerinin, kişisel verilerin arşivlendiği bölgelere giremez.
- Çalışanlar ve ilgili üçüncü kişiler, şirket bilgilerinin, kişisel verilerin nerede, nasıl saklanacağı ve alınması gereken önlemler hakkındaki talimatnamelere/bilgilendirmelere uymalıdırlar.

Önlemler;

- İşyerine mahsus bilgilerinin ve kişisel verilerin bulunduğu belge ve kayıtların kopyaları, yazıcı çıktıları vb. uygun dosya dolaplarında saklanır.
- Yeniden oluşturulamayan bilgiler, kişisel veriler yetkisiz erişim ve doğal zararlardan korunaklı bölgelerde depolanır.
- Bilgisayar diskleri kilitli bir dolapta ya da masada saklanır, işyerine mahsus bilgilerin ve kişisel verilerin bulunduğu bilgisayar diskleri ise özel dolaplarda kilit altında tutulur
- Düzenli olarak bilgisayarda saklanan bilgiler ve kişisel veriler yedeklenerek bilgisayarda oluşabilecek herhangi bir arıza durumuna karşı önlem alınır.
- İşyerine mahsus bilgiler ve kişisel veriler, işveren tarafından onaylanmış, şifreli erişime olanak sağlayan güvenlik programı tarafından korunan bir sabit diske kaydedilir.
- İşyerine mahsus bilgilerin ve kişisel verilerin açıklanmasında, dağıtımında, aktarımında düzenlenmesinde ve herhangi bir önemi kalmamış işyerine mahsus bilgilerin ortadan kaldırılmasında, mevzuat ve işyerinde belirlenmiş talimatlara uyulur.
- İşyerine mahsus bilgilerin ve kişisel verilerin bulunduğu sabit disk ve harici diskler düzgün bir şekilde silinir.
- İşyerine mahsus bilgi ve kişisel veriler yetkisiz erişimden korunur.
- İşyerine mahsus bilgilerin ve kişisel verilerin saklandığı bölgelere ait giriş kartları ya da anahtarları kimseye ödünç verilemez, kimseyle paylaşılamaz, bunlar başkalarının erişebileceği yerlere bırakılamaz.
- Sisteme erişim için, tahmin edilmesi zor şifreler seçilir ve bu şifreler, amirler dahil hiç kimseyle paylaşılamaz. Şifreler hiçbir zaman kolayca erişilebilecek bir yere yazılamaz ve belirli periyotlarla değiştirilir.

Çalışanlar işyerinde elektronik ortamda saklanan bilgileri ve kişisel verileri korumak için, bilgisayarlarının başından ayrıldıkları zaman, bilgisayarlarını şifreli konumda bırakırlar. Bütün bilgisayarlar, çalışanların işte olmadığı günlerde kapalı olur ya da ağ erişimi bulunmaz halde bırakılır.

Ekranlar, yetkisi olmayan insanların bilgilere ve kişisel verilere ulaşmasını engelleyecek şekilde yerleştirilir. Ekranlar, yoğun olan bölgelerin zıt yönüne konulur. Şüpheli duyulan ya da gerçekleştiğinden emin olunan bilgi güvenlik sorunları, hemen araştırılmak üzere amirlere/yetkilendiren kişiye bildirilir.

II. BİLGİSAYAR, İNTERNET, E-POSTA KULLANIMI

1. İNTERNET KULLANIMI GENEL PRENSİPLER

- Şirket çalışan personel ve danışmanlar, Görev Tanımları ve Sözleşmelerde tanımlı görevlerini yerine getirilebilmek için çalışmalarına destek olacak şekilde kendilerine sağlanacak Şirket kaynaklarını kullanarak internete erişebilirler,
- Bilgi İşlem Bölümü, İnternet erişimi sistemlerini kurmak, korumak, serviste tutmak ve belirli bir hizmet seviyesini sağlamaktan sorumludur. Şirket bünyesindeki grup şirketler ve Genel Müdürlük dışındaki birimlerde Bilgi İşlem Bölümü'ne bağlı Bilgi İşlem Yönetmenleri tarafından uygun programlar kurularak kullanıcıların internet erişimleri sağlanmaktadır,
- Bilgi İşlem Bölümü, gerekli durumlarda şirket bünyesindeki birimlerde kurulu olan sistemler gönderimin hızlandırılması amacıyla internet trafiği üzerinde kısıtlamalara gider ve kullanıcıların kullanım kapasitelerini düşürebilir,
- Şirket networkü üzerinden geçen her türlü bilgi, kişisel veri başka bir kişi/kurumun malı olduğu kesinleştirilmediği sürece, Şirket malı olarak kabul edilmektedir. Şirket, kendisine ait olan her türlü bilginin ve kişisel verilerin açıklanmasını, çoğaltılmasını, değiştirilmesini, saptırılmasını, yok edilmesini, kaybedilmesini, yanlış kullanılmasını, çalınmasını veya yetkisiz olarak erişilmesini yasaklamıştır,
- Üretkenliği artırıcı bir araç olarak sunulan İnternet erişimi ve elektronik posta servislerinin iş amacıyla kullanımı Şirket içerisinde yaygınlaştırılmaya çalışılmaktadır,
- Personel, Şirket ve Şirket'in yetkilendireceği kişiler tarafından internet kullanımının, hangi sitelere girdiğinin sistemde bulunan ara yüz sayesinde görülebileceğini ve kontrol edilebileceğini bilir. Bu hususun 5237 Sayılı Türk Ceza Kanunu'nun 132. Maddesi ve devamı maddelerinde yer alan özel hayatın gizliliğini ihlal suçu teşkil etmeyeceğini bilerek, söz konusu hususuna rıza gösterir.

2. BİLGİSAYAR KULLANIMINDA PERSONELİN UYMAK ZORUNDA OLDUĞU KURALLAR

2.1 Şirket personeli ve danışmanların, Mevzuat (Kalite Yönetim Sistemi), diğer şirket kuralları ve yürürlükteki Türkiye Cumhuriyeti yasalarına uygun hareket etmeleri gerekmektedir,

2.2 Sistemi gereksiz meşgul edecek, internet trafiğini gereksiz yere artıracak, müzik ve resim dosyaları, oyunlar, filmler ve benzeri programların (zip, rar, mpg, mpeg, avi, exe, com, mp3 vb. uzantılı dosyalar) internetten indirilmesi yasaktır,

2.3 Her türlü sohbet ve sosyal medya programının (MSN, Facebook, Twitter, Instagram ICQ, IRQ vb.) kullanıcılar tarafından bilgisayarlarda kurulması, kullanılması veya internet siteleri üzerinden kullanılması kesinlikle yasaktır. Sohbet, kumar, arkadaşlık, pornografi vb. sitelere erişim Bilgi İşlem Bölümü tarafından engellenmiş

durumdadır (İnternette bulaşan virüsler, çoğunlukla bu tür programlar aracılığıyla sisteme zarar vermektedir),

2.4 Şirket personeli ve danışmanların, Görev Tanımları ve Sözleşmelerde tanımlı görevlerini yerine getirilebilmek için çalışmalarına destek olacak şekilde İnternet aracılığı ile dağıtılan bazı ücretsiz sürüm programlarını kullanmak istemeleri halinde Bilgi İşlem Bölümü yetkililerine başvurmaları ve yazılı onay almaları gerekmektedir. Bu tür programların internet üzerinden indirilmesi, kurulması sadece Bilgi İşlem Bölümü personeli tarafından yapılacaktır. Bu tür programlar konusunda, Şirket' e zarar verecek ya da tanımlanan işin yerine getirilmesine katkısı olmayacak şekilde kullanım yapılmamalıdır,

2.5 Şirket personeli ve danışmanların, şirket içinden internet üzerinden sadece HTTP,HTTPS, SMTP servisine erişmelerine izin verilmektedir. Diğer servisleri kullanmak için Bilgi İşlem Bölümü'ne başvurmaları gerekmektedir. Şirket çalışanlarının ve danışmanlarının kullanmış oldukları bilgisayarlarda İnternet üzerinden farklı servis hizmeti veren programların (FTP, WEB, PROXY, NET vb. servisler) kurulması ve/veya çalıştırılması yasaktır,

2.6 Şirket personeli ve danışmanların, dışardan şirket içindeki sistemlere internet üzerinden bağlanmaları için VPN sistemini kullanmaları gerekmektedir. Bunun için Bilgi İşlem Bölümü'ne başvurmaları ve VPN kullanıcı kimliği ve şifresi almaları gerekmektedir,

2.7 Korsan yazılım, çalıntı şifre, çalıntı kredi kartı numaraları ve uygunsuz yazılı / grafik malzemenin herhangi bir şekilde indirilmesi, alışverişinin yapılması ve saklanması kesinlikle yasaktır,

2.8 Şirketin malı sayılan her türlü bilgi, doküman ve/veya yazılımın, iş amaçlı kullanım dışında, İnternet üzerinden satılması veya Şirket dışındaki üçüncü kişilere herhangi bir sebeple gönderilmesi kesinlikle yasaktır,

2.9 Şirket şirket içi kullanımı için hazırlanmış Şirket'in müşterileri ile ilişkilerini veya şirket imajını etkileyecek, herhangi bir bilgi, dosya veya duyurunun (iş potansiyelleri, birim maliyetleri, fiyatlar, yatırımlar, ihale bilgileri vb.) İnternet üzerinden açıklanması veya dağıtılması kesinlikle yasaktır,

2.10 Şirket' e ait önemli bilgilerin yetkisiz kişilere verildiği veya açıklandığı tespit edildiğinde veya bu konuda şüphe olduğunda konu Bilgi İşlem Müdürü ile zaman geçirilmeden paylaşılmalıdır.

2.11. Personel, Şirket'in (örneğin)Turkcell İletişim Hizmetleri A.Ş. ile Mobilparkma İletişim ve Bilişim Hizmetleri San. ve Tic. A.Ş: ile hizmet sözleşmesi olduğunu bilir, bu bağlamda gerekli gördüğü takdirde Şirket ve Şirket'in yetkilendireceği kişiler bilgisayar içeriğinde bulunan her türlü bilgi, belge, materyallerin sistemde bulunan ara yüz sayesinde görülebileceğini ve kontrol edilebileceğini bilir. Bu hususun 5237 Sayılı Türk Ceza Kanunu'nun 132. Maddesi ve devamı maddelerinde yer alan özel hayatın gizliliğini ihlal suçu teşkil etmeyeceğini bilerek, söz konusu hususuna rıza gösterir.

3. ELEKTRONİK POSTA KULLANIMI GENEL PRENSİPLER

3.1 Şirket personeli, Görev Tanımlarında tanımlı görevlerini yerine getirilebilmek için çalışmalarına destek olacak şekilde kendilerine sağlanacak şirket kaynaklarını kullanarak elektronik posta gönderebilir/alabilir,

3.2 Tüm Şirket personeli için bir elektronik posta kutusu yaratılmaktadır. Bilgi İşlem Bölümü tarafından her kullanıcı için kişiye özel bir kullanıcı adı ve şifre verilir. Personel, bağlı olduğu Direktörlük/Müdürlük, görev/sorumluluğuna bağlı olarak ilgili elektronik posta dağıtım gruplarına dâhil edilir; bu gruplar dışında kullanıcının eklenmesi gereken bir dağıtım grubu varsa özel olarak belirtilmesi gerekir,

3.3 Hiçbir koşulda kişisel şifreler, yetkili Bilgi İşlem Bölümü haricindeki personele gösterilmemeli / paylaşılmamalıdır. Şifre sadece kullanıcı tarafından bilinir ve korunması tamamıyla kullanıcının sorumluluğundadır. Bilgi İşlem Bölümü, şifre kullanımından doğacak problemlerden kesinlikle sorumlu değildir. Aksi durumlarda, şifresini paylaşan kişi şifreyi öğrenen kişinin kendisi adına yapacaklarının sorumluluğunu kabul etmiş sayılır. Kullanıcıların bilgi paylaşımını elektronik posta yönlendirme, dosya sunucuları ve diğer yetkilendirilebilir bilgi paylaşımı mekanizmalarını kullanarak ,yapmaları gerekmektedir. Yetkisiz kişilerin kullanıcı şifrelerini tespit etmesini engellemek için kullanıcıların tahmin etmesi zor şifreler kullanmaları gerekmektedir,

3.4 Personelin işten ayrılması durumunda, Bilgi İşlem Bölümü'ne, elektronik posta ile bilgi verilir ve ilgili elektronik posta hesabı kapatılır. Bilgi İşlem Bölümü, Bölüm sorumlusunun talepte bulunması durumunda, elektronik postanın başka bir kullanıcıya yönlendirilmesi ve/veya kullanımının geçici olarak kısıtlanması gibi faaliyetleri gerçekleştirilebilir,

3.5 Tüm elektronik posta sistemleri ve bu sistemler üzerinde oluşturulan, tutulan ve/veya saklanan mesaj, bilgi ve dosyaların hepsi (yedeklenen kopyaları dâhil) Şirket malı olarak kabul edilir,

3.6 İş talebi, iş takip sonucu vb. belirli bir sürecin yaşandığı konular hakkındaki gönderilerde önceki elektronik postalar için İlet seçeneği seçilerek elektronik posta oluşturulur,

(Bu gibi durumlarda önceki elektronik postalarda gönderiyi ilettiğiniz kişinin, iş güvenliği nedeniyle görmesini istemediğiniz bilgileri konunun özüne zarar vermeyecek ölçüde silebilirsiniz.)

3.7 Harici kişi ve kurumlara gönderilen elektronik postalarda işin gereği ile ilgili bilgilerin dışında, şirketin güvenliği ile ilgili bilgiler verilmemelidir.

3.8 Elektronik postayı gönderen personelin imzasının; imza alanında da mutlaka unvan, Şirket adı ve iletişim bilgilerinin bulunması gerekmektedir.

3.9 Çalışanlara ait kişisel diğer elektronik posta adreslerinin elektronik posta okuma/gönderme programlarına tanıtılması ve kullanılması yasaktır,

3.10 Şirket personelinin, gönderebileceği elektronik posta boyutu standardı (örneğin)20 MB olarak belirlenmiştir. Ancak gerekli durumlarda Bilgi İşlem Bölümü'ne başvurularak elektronik posta boyutu artırılabilir,

3.11 Çalışanlara dışardan gelecek elektronik postaların boyutunda herhangi bir kısıtlamaya gidilmemekle birlikte internet ve network trafiğine engel olacak bir durum olduğunda Bilgi İşlem Bölümü posta boyutlarına bir kısıtlama getirme hakkına sahiptir,

3.12 Şirket, personelinin kişisel – makul mahremiyet isteklerine saygı gösterilmesine büyük önem vermektedir. Bununla birlikte, Bilgi İşlem Bölümü, elektronik posta sistemlerini kurmak, korumak ve serviste tutmaktan sorumludur. Bunu sağlamak için bazen elektronik posta mesajlarının açıklanması, paylaşılması veya durdurulması gerekebilir,

3.13 Bilgi İşlem Bölümü elektronik posta mesajlarının gizliliğini/mahremiyetini kendi kontrol ve sorumluluğu dışındaki sistemlere gönderildiği andan itibaren garanti edemez. Kullanıcıların, teknolojiye bağlı olmakla birlikte, gönderilen elektronik posta mesajlarının gönderilen kişi tarafından yönlendirilebileceği, durdurulabileceği, yazdırılabileceği, saklanabileceği ve değiştirilebileceğinin farkında olduğu varsayılmaktadır. Elektronik posta mesajlarının içeriğinin incelenmesi Bilgi İşlem Bölümü'nün politikaları arasında yer almamaktadır. Bununla birlikte, elektronik posta sistemlerinin kullanımı, araştırma aktivitelerinin desteklenmesi sebebiyle izlenecektir.

3.14 Şirket personelinin, elektronik postaları kendi bilgisayarlarındaki Kişisel Klasör kısmında tutulmaktadır. Gerekli durumlarda Bilgi İşlem Bölümü'ne başvurularak sistem sunucusu üzerinde elektronik postaların tutulması belli bir kota sınırı altında kalmak koşuluyla sağlanabilir.

3.15 Danışmanlar için sistem üzerinde elektronik posta kutusu yaratılmaz. Yaratılması çok gerekli görülüyor ise Danışman'ın iş yaptığı birimin bağlı olduğu Direktör/Müdür'ün bu talebi onaylaması gerekmektedir.

3.16 Bilgi İşlem Bölümü elektronik posta sisteminin kullanımı, güvenliği ve gerekli teknik altyapı ve desteği sağlamakla yükümlüdür.

3.17 Personel, Şirket ve Şirket'in yetkilendireceği kişiler mail trafiğinin ve içeriklerinin sistemde bulunan ara yüz sayesinde görülebileceğini ve kontrol edilebileceğini bilir. Bu hususun 5237 Sayılı Türk Ceza Kanunu'nun 132. Maddesi ve devamı maddelerinde yer alan özel hayatın gizliliğini ihlal suçu teşkil etmeyeceğini bilerek, söz konusu hususuna rıza gösterir.

4. ELEKTRONİK POSTA KULLANIMININ ETKİN OLARAK GERÇEKLEŞTİRİLEBİLMESİ İÇİN PERSONELİN UYMASI GEREKEN TEMEL KURALLAR

Elektronik postalar tartışmasız bir şekilde bir iletişim aracı olup hatta gerektiğinde çoklu iletişimin en kolay şeklidir. Bu nedenle tüm çalışan ve geçici danışmanların, aşağıdaki *bilgilendirme (CC ve BCC) kurallarına* uymaları gerekmektedir.

- Elektronik posta ve web sayfaları adreslerinde Türkçe karakterler (ç, ş, ı, ö, ü, ğ) kullanılmaz.
- Elektronik postalarınızı, Konu kısmı boş şekilde göndermeyiniz; içeriğin ne hakkında olduğunu bildiren bir satırın olması Gönderilere tekrar bakma gereği duyulduğunda hem sizin hem alıcının işini kolaylaştırır. Konu kısmına yazacaklarınız içeriğe uygun anahtar kelimeler veya kısa bir tanım olmalıdır.
- Gönderdiğiniz elektronik postalara ekleyeceğiniz dosyaların uygun boyutlu (örneğin, 20 megabayt) küçük olmasına dikkat ediniz.

- Eğer elektronik posta ile büyük boyutlu dosyalar eklenecek ise SIKIŞTIRMA (WINRAR, WINZIP, vb..) programını kullanarak boyutunu küçültünüz. Bu eklentiler içinde hangi dosyaların bulunduğunu ve bu dosyaları hangi programlarla açılabilceğini açıklarsanız virüs olduğu şüphesi duyulmaz.
- Aldığınız elektronik postayla beraber gelen eklentileri açarken dikkatli olmalısınız. Çünkü virüsler en sık bu şekilde bulaşıyor. Siz de başkalarına dosya göndereceğiniz zaman virüs taramasından geçirdikten sonra gönderiniz. Uzantısı. .exe, .bat, .com olan dosyaları (göndericisini tanıyor olsanız bile) asla çalıştırmayınız.
- Çoğu virüs elektronik posta okunduğu anda aktif olduğu için, Outlook, Outlook Express programında ön izleme penceresini aktif yapmayınız.
- Gönderdiğiniz elektronik postaların sizi yansıttığını unutmayın; gönderdiğiniz kişiler sizi tanımıyor veya görmüyor olabilir; ancak kullandığınız yazı dilinin ve biçiminin sizin hakkınızda ipuçları vereceğini unutmayın. Elektronik postalarınızın diline, imlâ ve yazım kuralları ile genel ahlâk kurallarına uygun olmasına dikkat ediniz.
- Elektronik postalarınızı açık ve öz olarak yazmalısınız.
- Elektronik postalarınızın içeriği normal cümle düzeni içinde olmalı, gerektiği yerlerde büyük ve küçük harfler kullanılarak yazılmalıdır. Büyük harf kullanımının elektronik yazışma dilinde bağırma, kızma anlamına geldiğini unutmayın.
- Elektronik posta kutunuzu her gün kontrol edin ve postalarınızı limitinizi aşacak kadar sistemde tutmayınız. Gereksiz elektronik postaları, posta kutunuzdan silmelisiniz. Sildiğiniz elektronik postalar silinen klasöründe saklandığı için bu klasörü de periyodik olarak boşaltmanız gerekmektedir.
- Elektronik posta olarak yanıt verirken cevap verdiğiniz gönderiden yeteri kadar alıntı yapınız. Tüm gönderiyi olduğu gibi alarak elektronik postanın uzunluğunu artırmayınız. Orijinal gönderinin konuyla ilgisiz yerlerini siliniz.
- Size özel yazılmış bir elektronik postayı, gönderi sahibinin haberi olmaksızın başkasına göndermeyiniz.
- Çok sayıda kişiye gönderdiğiniz gönderileri CC (Carbon Copy) ile değil BCC (Blind Carbon Copy) ile gönderiniz. Böylece alıcıların birbirlerinin adreslerini görmesine engel olursunuz.
- Elektronik postalarınızda kredi kartı numarası, herhangi bir şifre, vb. özel bilgileri çok gerekmedikçe yazmayınız.
- Hiç bir zaman elektronik postanızın sadece siz ve gönderdiğiniz kişi tarafından okunacağını zannetmeyiniz. Telefonda söyleyemeyeceğiniz şeyleri elektronik posta ile de göndermeyiniz.

- Şifrenizi kimseye vermeyiniz ve belli periotlarda deęiřtiriniz (45 ya da 60 günde bir).
- Elektronik posta aracılıęıyla size verilen iřleri etkin olarak takip edebilmek için izle seęeneęini kullanabilirsiniz. İzle seęeneęini kullanarak ilgili iř için teslim tarihinizden belirli bir süre önce size sistem tarafından hatırlatılma yapılmasını saęlayabilirsiniz.
- Elektronik postanızda Araçlar-Seęenekler-Tercihler-elektronik posta Seęenekleri adresine girerek gönderdięiniz elektronik postaların gönderdięiniz kiřilerce teslim alındıęını ve/veya okunduęu bilgilerinin yine elektronik posta aracılıęıyla size bildirilmesini saęlayabilirsiniz.
- Elektronik postanızda Araçlar-Seęenekler- Posta Seęenekleri adresine girerek Gönderdięiniz elektronik postalarda otomatik olarak çıkacak ve sizi tanımlayacak imzanızı oluřturabilirsiniz. İmzanızda Ad Soyad – Bölüm – unvan – telefon bilgilerinizin bulunması gerekmektedir.
- Elektronik posta gönderilerinizin önem seviyesinin Yüksek olduęunu belirtmek için Yüksek Önem (kırmızı ünlem iřareti) butonunu iřaretlemelisiniz.
- İř yerinizde deęilken size gelen elektronik postaları otomatik olarak cevaplandırmak ve elektronik posta gönderenleri bilgilendirmek için Araçlar – İřyeri Dıřı Yardımcısı seęeneęini kullanarak hazırlayacaęınız otomatik gönderilerden faydalanabilirsiniz.
- Elektronik posta – Takvim seęeneęini kullanarak ve kiřisel hatırlatıcı notlar oluřturarak iřlerinizi takip edebilirsiniz.

5. ELEKTRONİK POSTA KULLANIMINDA PERSONELİN UYMAK ZORUNDA OLDUęU KURALLAR

Personel; iře bařladıęı ve elektronik posta kullanmaya bařladıęı andan itibaren,

5.1 Őirket elektronik posta servisini kullanarak ileri sürdüęü kiřisel düşünce, ifadelerin ve ekledięi dosyaların sorumluluęunun kendisine ait olduęunu ve Őirket' in bu elektronik posta ve dosyalardan dolayı hiębir Őekilde sorumlu tutulamayacaęını,

5.2 Elektronik posta kullanımı sırasında, sistem geneline zarar verecek veya Őirket' in bařka kiři ya da kuruluřlarla hukuki anlaşmazlıęa sokacak herhangi bir yazılım veya materyal bulunduramayacaęını, paylařamayacaęını ve cezai bir durum doęarsa tüm cezai sorumlulukları üstüne aldıęını,

5.3 Elektronik posta servisinin kullanımı sırasında kaybolacak ve/veya eksik alınacak, yanlıř adrese gönderilecek bilgi, mesaj ve dosyalardan Őirket' in sorumlu olmayacaęını,

5.4 Elektronik posta adresi verilerinin Bilgi İřlem Bölümü'nün ihmali görülmeden yetkisiz kiřilerce okunmasından (kiřinin bilgilerini bařka kiřiler ile paylařması, sistemden ayrılırken çıkıř yapmaması vb.) dolayı gelebilecek zararlardan ötürü Őirket' in sorumlu olmayacaęını,

5.5 Tehdit edici, ahlak dışı, ırkçı, ayrımcı, Türkiye Cumhuriyeti Yasalarına, vatandaşı olduğu diğer ülkelerin yasalarına ve uluslararası anlaşmalara aykırı mesajlar göndermemeyi,

5.6 Ortama eklenecek yazışmaların, konu başlıklarının, genel ahlak, görgü ve hukuk kurallarına uygun olmasını,

5.7 Diğer kullanıcıları taciz ve tehdit etmemeyi,

5.8 Diğer kullanıcıların servisi kullanmasını etkileyecek şekilde davranmamayı,

5.9 Diğer kullanıcıların bilgisayarındaki bilgilere ya da yazılıma zarar verecek bilgi veya programlar gönderme meyi,

5.10 Şirket elektronik posta servisini kullanarak elde edilen herhangi bir kayıt veya elde edilmiş malzemelerin tamamıyla kullanıcının rızası dâhilinde olduğunu, kullanıcı bilgisayarında yaratacağı arızalar, bilgi kaybı ve diğer kayıpların sorumluluğunun tamamıyla kendisine ait olduğunu, servisin kullanımından dolayı uğrayabileceği zararlardan dolayı Şirket' den tazminat talep etmemeyi,

5.11 Kurallara aykırı davrandığı takdirde Şirket tarafından gerekli müdahalelerde bulunma, kişiyi hizmet dışına çıkarma ve üyeliğine son verme hakkına sahip olduğunu,

5.12 Kanunlara göre postalanması yasak olan bilgileri postalamamayı ve zincir posta (chain mail), yazılım virüsü vb. gibi gönderilme yetkisi olmayan postaları dağıtmamayı,

5.13 Elektronik posta sisteminde kullanıcı adıyla yapacağı her türlü işlemde bizzat kendisinin sorumlu olduğunu, Kabul etmiş sayılmaktadır.

Kişilerin bu kurallara uymalarını izlemek Bilgi İşlembölümünün görevidir.

İŞVEREN
Kaşe ve İmza

ÇALIŞAN
Ad Soyad ve İmza
Okudum,anladım (el yazısı ile)