SİMİN İŞ SAĞLIĞI VE GÜVENLİĞİ EĞİTİM VE DANIŞMANLIK TİC. LTD. ŞTİ.

PERSONEL BİLGİ TEKNOLOJİLERİ KULLANIM POLİTİKASI

Adres : Bağlarbaşı Mah. Refahevler Sokak No: 2/2
MALTEPE /İSTANBUL
Telefon :+90(216) 519 83 12
Web : http://simin.com.tr/
E-mail :simin@simin.com.tr

İÇİNDEKİLER

SİMİN İŞ SAĞLIĞI VE GÜVENLİĞİ EĞİTİM VE DANIŞMANLIK TİC. LTD. ŞTİ.
PERSONEL BİLGİ TEKNOLOJİLERİ KULLANIM POLİTİKASI

Yayınlanma Tarih	:
Gizlilik	: GENEL KULLANIM
İlgili Doküman	: BT Güvenlik Politikası
Sahibi ve güncelleme sorumlusu	: Bilgi Teknolojileri Departmanı
Görev ve sorumluluklar	: Yönetim, Yönetim Temsilcisi, Tüm çalışanlar

Kısaltmalar:

BT: Bilgi Teknolojileri / IT
P2P: Uçtan uca bağlantı
VPN: Sanal özel ağ
Wi-Fi: Kablosuz ağ

1. Amaç:

Firmamızın bilişim sistemlerinde çok önemli bilgiler olup bu bilgilerin güvenliği, gizliliği ve kişisel mahremiyetin korunması büyük önem arz etmektedir. Ağa bağlı olan herhangi bir bilgisayardaki güvenlik açığı firmamızın bütün bilişim sistemlerinin güvenliğini riske atmasına sebep olabilir.

2. Kapsam:

a) Firmamızın bilişim sistemlerinin güvenliğinde herhangi bir aksamaya mahal verilmemesi için genel sistem ve kullanım seviyesinde alınmış olan güvenlik tedbirleri yanında çalışanlarımızın da bu hususta titizlikle uyması gereken birtakım kurallar vardır. Bu kurallara bütün firma çalışanları uymak zorundadır.

b) Bu kurallara uyulmadığı takdirde oluşabilecek her türlü zarar ve olumsuz sonuçlardan kullanıcı sorumludur. Uyulması gereken kurallar aşağıda belirtilmiştir.

3. E-Posta Kullanım Kuralları

a) Firmanın e-posta sistemi taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için, kötü amaçlı ve kişisel çıkar amaçlı kesinlikle kullanılamaz.
b) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
c) Kişisel kullanım için internetteki listelere üye olunması durumunda firma e-posta adresleri kullanılmamalıdır.
ç) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır. Aynı zamanda firma e-posta adresi şirket içi ve dışı başka kullanıcılara spam, phishing mesajlar göndermek için kullanılamaz.

d) Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak herhangi bir işlem yapılmaksızın derhal silinmelidir.
e) Çalışanlar, e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb.) ve firma içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta gönderemezler.
f) Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
g) Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
ğ) Firma çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajlarını yanıtlamalıdır.
h) Firma çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemekten sorumludurlar.
ı) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu e-postalar virüs, e-posta bombaları ve Truva atı gibi zararlı kodları içerebilirler.
i) Firma çalışanları gönderdikleri, aldıkları veya sakladıkları postalarda kişisellik aramamalıdır. Yasa dışı ve hakaret edici e-posta haberleşmesi yapılması durumunda yetkili kişiler önceden haber vermeksizin e-posta mesajlarını denetleyebilir ve kullanıcı hakkında yasal işlemler başlatabilir.
j) Firmaya ait hiçbir “Hassas” veya “Gizli” doküman, açık metin olarak kullanıcıların kendilerine ait özel e-posta adresleri de dâhil olmak üzere herhangi bir kişiye gönderilemez.
k) Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludurlar. Şifrelerinin kırıldığını fark ettikleri andan itibaren yetkililerle temasa geçip durumu haber vermekle yükümlüdürler.

4. Şifre Politikası

a) Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, taşınabilir bilgisayar, masaüstü bilgisayar vb.) en az 6 ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her dört ayda birdir.
b) Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
c) Şifreler başkası ile paylaşılmamalı, kâğıtlara ya da elektronik ortamlarda yazılmamalıdır.
ç) Şifrelemede, küçük ve büyük karakterlere (Örnek, a-z, A-Z), hem rakam hem de noktalama karakterleri ve ayrıca harfler (örnek:0-9 !@^+%&*()_+|=%&/()?,./) bulunmalıdır.
d) En az sekiz adet alfa numerik (harf, sayı ve noktalama işareti) karaktere sahip olmalıdır.
e) Herhangi bir dilde argo kelime olmamalıdır.

f) Aile isimleri kullanılmamalıdır.
g) Herhangi bir kişiye telefonda şifre verilmemelidir.
ğ) Şifreler aile bireyleri dâhil hiç kimseyle paylaşılmamalıdır.
h) Şifreler, işten uzakta olduğunuz zaman iş arkadaşlarınıza verilmemelidir.
ı) Bir kullanıcı adı ve şifresinin birim zamanda birden çok bilgisayarda kullanılmamalıdır.
i) Şifre kırma ve tahmin etme operasyonları BT tarafından belli aralıklarla yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.
j) Şirket maili üzerinden atılacak her türlü doküman sıkıştırılıp şifrelenmelidir. Şifre aynı mail üzerinden değil telefonla arayarak iletilir.
k) Şirket içinde USB kullanımında bir evrakın USB'ye depolanması gerekliyse bunun sıkıştırılıp şifreli bir şekilde depolanması gereklidir. Yukarıda belirtilen USB ya da herhangi bir taşınabilir aygıtta geçerli olup sadece zaruri ve BT' nin bilgisi dâhilinde yapılmalıdır.

5. Antivirüs Politikası

a) Bütün bilgisayarda Antivirüs yazılımı yüklü olmalıdır ve otomatik olarak güncellenmelidir.
b) Antivirüs yazılımı yüklü olmayan bilgisayarlar ağa bağlanmamalıdır.
c) Zararlı programları (örnek: virüsler, solucanlar, Truva atları, e-posta spam vb.) firma bünyesinde oluşturmak ve dağıtmak yasaktır.
ç) Hiçbir kullanıcı herhangi bir sebepten dolayı Antivirüs programını sistemden kaldıramaz.
d) Kurulumu yeni yapılan her yeni işletim sisteminde Antivirüs programı yüklü olmak zorundadır.

6. İnternet Kullanım Politikası

a) Hiçbir kullanıcı P2P bağlantı yoluyla internetteki dosya indirme ve yükleme servislerini kullanamayacaktır. (Örnek: *Kaza, torrent, imesh, edonkey* vb.)
b) Bilgisayar ağında firma görüşmeleri haricinde *ICQ, MIRC, Messenger* vb. mesajlaşma ve sohbet programları gibi *Chat* programlarının kullanılmaması ve bu *Chat* programları üzerinden dosya alışverişinde bulunulmaması gerekmektedir
c) Hiçbir kullanıcı internet üzerinden iş ile ilgili haberleşme amacının dışında olarak *Multimedya Streaming* (video paylaşımı ve ses/görüntü yayıncılığı) yapamayacaktır.
ç) Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır. (Örnek: *Facebook, Youtube*)
d) İş ile ilgili olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek (*upload*) ve indirmek (*download*) etmek yasaktır.
e) İnternet üzerinden BT birimi tarafından onaylanmamış yazılımlar indirilemez ve firma sistemleri üzerinde bu yazılımlar kurulamaz ve kullanılamaz,

f) Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemesi ve dosya indirimi yapılması yasaktır.
g) Bilgisayarların işletim sistemleri için büyük ölçüde tehdit ettiği için internet üzerinden ekran koruyucu, masaüstü resimleri, yardımcı program olduğu belirtilen araçlar gibi her türlü programların indirilmesi ve kopyalanması yasaktır.
ğ) Üçüncü şahısların firma içerisinden internetini kullanmaları BT sorumlusunun izni ve bu konudaki kurallar dâhilinde gerçekleştirilebilecektir.
h) Firma tarafından, iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik çalışması yapılır.

7. Temiz Masa Temiz Ekran Politikası

a) Çalışma saatleri sonunda masa üstünde herhangi bir doküman bırakılmaz, genellikle ofis masalarının parçası olan kilitli çekmecelere ya da dolaplara kaldırılır.
b) Ofisten uzun süreli ayrılmalar öncesinde, çalışma masası ve çevre ünitelerinde evrak temizliği yapılır. Önemli doküman dolaplara ve kilitli çekmecelere kaldırılır. Personel, fiziki dokümanları olası tehlikelere karşı (Sıvı dökülmesi, yanması, tahribe uğraması) korumakla yükümlüdür,
c) Şifre ve kullanıcı adı yazılı küçük kâğıtlar çalışma masası üzerinde veya çevresinde bırakılmaz.
ç) Masa üstü doküman sayısını artırmamak için mümkün olduğu kadar, elektronik dokümanların yazıcıdan çıktılarının alınmamasına dikkat edilir.
d) Basılı dokümanların “lazım olur” diye masa üstünde biriktirilmesi yerine, bu dokümanların tarayıcılardan elektronik kopyalarının alınması ve bilgisayarda yedeklenmesi, dokümanın kendisinin ise ya imha edilmesi ya da dosyalanması daha uygundur.
e) Kâğıtların çöp kutularına atılması yerine, kâğıt imha makinelerinde kırpılmasına dikkat edilir.
f) Kısa süreli ayrılmalarda dahi, cep telefonu , USB bellek, harici sabit disk, CD, DVD gibi eşyalar çalışma masası üzerinde bırakılmamalıdır.
g) Kısa süreli ayrılmalarda masa üstünde değerli bilgileri sahip olmayan doküman bırakılmaz, bunlar kilitli çekmecelerde saklanır.
ğ) Masa üzerinde kartvizit kutuları, kişisel ajandalar, banka hesap defterleri, çek defterleri gibi değerli bilgilere sahip doküman bırakılmaz, bunlar kilitli çekmecelerde saklanır.
h) Dokümanların yanı sıra, bilgisayar ekranları da çalışma masasından kısa süreli ya da uzun süreli ayrılırken ya kapatılmalı veya şifre korumalı ekran koruyucu aktif hale getirilmelidir.
ı) Masa çekmecelerinin anahtarları, ev ve araba gibi özel anahtarlar, kasa anahtarları masa üzerinde bırakılmamalıdır.

8. Sosyal Mühendislik Saldırılarından Korunma Politikası

a) Teknoloji kullanımından çok insan zafiyetlerini hedef alarak çeşitli ikna ve kandırma yöntemleriyle bilgi edinme yoludur.
b) Sahte senaryolar uydurmak, güvenilir bir kaynak olduğuna ikna etmek (*phishing*), Truva atları, güvenilir bilgi karşılığında para, hediye vb. önermek, güven kazanarak bilgi edinmek gibi saldırı yöntemleri kullanılır.
c) Kurum içerisinde, kurum dışında, hatta evinizde, sosyal mühendislik saldırılarına maruz kalabilirsiniz. Telefon, faks, e-posta, telekonferans gibi farklı iletişim ortamları için de aynı şey geçerlidir. Tehlike hiç ummadığınız bir anda hiç ummadığınız bir yerden gelebilir. Olağan dışı durumlarla karşılaştığınız zaman harekete geçmeden önce bir kez daha düşünün. Kendinizi büyük bir tuzağın içine düşmek üzere iken bulabilirsiniz.
ç) Tanımadığınız kişilerden gelen isteklere karşı temkinli davranın. Telefon ile arandıysanız, karşı tarafın telefon numarasını isteyin, Yüz yüze görüşme ise, adres ya da telefon bilgisini isteyin.
   Aşağıdaki durumlardan biri oluşursa görüşmeye derhal son verin:
   İsteğin yerine getirilmemesi durumunda kötü sonuçlar doğacağının vurgulanması,
   Sıra dışı taleplerde bulunulması,
   Soru sorduğunuzda rahatsız olunması,
   Yetkili olduğunun öne sürülmesi,
   Bildiğiniz konu ile ilgili isimlerin art arda sıralanması,
   Durumun acil olduğuna dair vurgu yapılması,
   İltifat edilmesi veya kur yapılması,
   Size özel bilginizi (örneğin şifreniz) kimseyle paylaşılmaması,
   Sistem yöneticisiniz,
   Yan masada oturan mesai arkadaşınız,
   Hatta yöneticileriniz,
   İstek talepleri bildiğiniz, tanıdığınız, güvendiğiniz e-posta ve telefon numarasından gelse bile, bilgisayar hesap ve şifrelerinizle ilgili bir bilgiyi paylaşmayın.
   E-postanıza gelen aldatıcı postaları açmayın. Açmış iseniz bile bu e-postada yollanan linklere tıklamayın, resimleri indirmeyin, e-postaları cevaplamayın.
   Hiçbir kurum ve internet sitesi yöneticisi sizin giriş bilgilerinize ihtiyaç duymaz, çünkü üyeliğiniz veya hesabınız üzerinde bir değişiklik ya da işlem yapabilmesi için hazırlanmış bir “site yöneticisi” (administrator) paneli vardır. Bu yüzden yönetici ya da site sahibi olduğunu iddia eden kişilere üyelik bilgilerinizi ve tabi ki şifrenizi vb. vermemelisiniz.
   Birisi size bir suç işlediğinizi veya ödül kazandığınızı düşündürerek telaşlı ya da heyecanlı bir ruh haline bürünmenizi sağlayıp, zayıf anınızdan faydalanmak istediğinde bilmelisiniz ki; hiçbir kamu görevlisi sizi bulunduğunuz durumdan kurtarmak için telefonda ya da e-posta yoluyla sizden para talep etmez ve yine aynı şekilde hiç kimse ödül vereceği kişiden kimlik bilgisini, belli bir hesaba ya da telefon numaranıza para yollamasını istemez.

d) Bilgisayarınızda korsan programlar, müzikler, videolar kullanmamalısınız. Kumar ve benzeri kötü amaçlı sitelere girmemelisiniz.

9. Mobil Bilgi İşlem Politikası

a) Telefonunuzu daima yanınızda bulundurun. Onu sahipsiz bırakmayın. Telefonunuzu her yerde sergilemekten kaçının. Araç ile seyahat ediyorsanız aracı terk ederken mobil cihazların yanınızda olduğundan emin olun.
b) Daima telefonunuzun güvenlik kilit kodunu ya da PIN kodlarını kullanın ve bunları sır olarak saklayın. Daima ön tanımlı fabrika ayarlarındaki şifre ve PIN kodları değiştirerek, bu kodları size özel kılın.
c) Telefonun fabrika ayarlarının ve işletim sisteminin ayarlarının jailbreak, rooting, kırdırmak gibi işlemler yaparak değiştirilmesi kesinlikle yasaktır. Bu akıllı telefonun siber saldırılara karşı daha duyarlı yaparken, işletmeci ve akıllı telefon tarafından sunulan güvenlik özelliklerini zayıflatmaktadır
ç) Uygulamaların, akıllı telefonlarınızda bulunan kişisel bilgilerinize erişme yetkisi konusunda dikkatli olmanız tavsiye edilir. Aksi halde indireceğiniz uygulama ile kişisel bilgileriniz (örneğin konum veriniz) üzerinde işlem yapılmasına izin vermiş olabilirsiniz. Ayrıca yüklemeden önce her uygulama için gizlilik ayarlarını kontrol ettiğinizden emin olmalısınız.
d) Bir uygulamayı indirmeden önce, uygulamanın yasal ve güvenilir olduğundan emin olmak için araştırma yapılmalıdır. Akıllı telefonlara indirilecek uygulamaları, işletim sisteminin resmi uygulama ortamından edinilmesi önemle tavsiye edilmektedir.
e) Akıllı telefonlarda, uygulama olarak edinilebilecek veya firma MDM kullanılarak kurulan uygulama ile telefonun GPS' i kapalı olsa bile, telefonunuzda depolanan tüm verilere uzaktan erişebilmeye ve söz konusu verileri silebilmeye imkân sağlamasıdır. Bu durumda telefonunuzu kaybettiğinizde, telefonunuz sessiz olsa bile bazı uygulamalar yüksek sesli bir alarmı aktif edebilir. Bu uygulamalar aynı zamanda telefonunuzu kaybettiğinizde daha kolay bulabilmenize yardımcı olabilir.
f) Kullanmadığınız zaman, Bluetooth, Wi-Fi ve diğer hizmetleri devre dışı bırakmalısınız.
g) Otomatik güncellemeleri etkinleştirerek, telefonunuzun işletim sistemini güncel tutmalısınız veya servis sağlayıcınızdan, işletim sistemi sağlayıcınızdan, cihaz üreticisinden ve uygulama sağlayıcınızdan gelen güncellemeleri kabul etmelisiniz. İşletim sisteminizi güncel tutarak, siber tehditlere maruz kalma riskini azaltabilirsiniz.
ğ) Eğer telefonunuzun veri şifreleme özelliği varsa bu özelliği kullandığınızdan emin olmalısınız. Böyle biz özellik yoksa veri şifreleyen uygulama kullanmanız tavsiye edilir. Telefonun çalınması ya da kaybolması durumunda veriler ele geçirilse bile ilgili şahıs tarafından kullanılamayacak ve anlaşılamayacaktır.
h) Telefonunuzun çalınması veya kaybolması durumunda, hattınızı kapatmak için firma Bilgi Teknolojileri bölümüne başvurun. Telefonunuzun ülkemizde kullanımını engellemek için durumu Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) (www.btk.gov.tr) bildirebilirsiniz.

ı) SIM kartını, ek hafıza kartını, pili ve telefonu bir işaretle fiziksel olarak ve yabancılar tarafından hemen fark edilmeyecek şekilde işaretleyin (çizin) (küçük bir işaret, harf ya da sayılar çizin ya da normal ışıkta görünmez olan mor ötesi boya kullanmayı deneyin).
i) SIM kartınızda, ek hafıza kartınızda ve telefonunuzun hafızasında hangi bilgileri kayıtlı tutulduğunun farkında olduğunuzdan emin olmalı ve hassas bilgileri telefonunuzda depolamamalısınız.
j) SIM ve ek hafıza kartınızı koruyunuz ve telefonunuzu servise verdiğinizde SIM kartınızı ve ek hafıza kartınızı orada bırakmadığınızdan emin olunuz.
k) 15 haneli seri no ya da IMEI numaranızı kaydedin. Bu telefonunuz kaybolduğunda ya da çalındığında telefonun izini sürmeye ve mülkiyetini korumaya yardımcı olur.
l) Internet Kullanım Politikasına telefon ve diğer taşınabilir cihazlarınızı kullanırken de bu kurallara uymalısınız.

10. Uzaktan Çalışma Politikası

a) Halka açık yerlerde ya da misafir olduğunuz firmalarda ortak internet (Wi-Fi) erişimi kullanıyorsanız VPN kullanmak gerekebilir.
b) Şifresiz herkese açık kablosuz ağ trafiği bu hizmeti bedava veren kişi tarafından dinleniyor olabilir. Halka açık ağ kullanımını kısıtlamalı ve onun yerine güvenebileceğiniz bir operatöre ait güvenli Wi-Fi veya kablosuz mobil bağlantı ağı kullanmalısınız.
c) Kişisel bilgisayarınızın dosya paylaşım özelliklerini kapalı tutmalı ve güvenlik duvarınız (*firewall*) her zaman açık (ON) durumda olmalıdır.
ç) Hassas bilgi içeren dosyaları bilgisayarınızda tutmayın. Tutmanız gerekiyorsa; Google Drive (bulut) ortamında tutmalısınız. Eğer lokal bilgisayarda tutmanız gerekiyorsa ki tavsiye etmiyoruz, hassas bilgilerinizi, disk şifreleme yazılımı ile korunan bir alanda saklamalısınız.
d) Cihazınızın çalınma ya da kaybolma riskine karşın firma uygulama ve sunucu hesapları ile ilişkili şifreleriniz bilgisayar üstünde yazılı olarak durmamalı ve böyle bir duruma maruz kaldığınızda zaman geçirmeden firma yetkililerine acil olarak haber vermelisiniz.

Uzaktan firma ağına bağlanarak çalışan kullanıcıların bilgisayarları belirli zamanlarda kontrol edilecektir. Bu kontroller aşağıdakileri kapsayacaktır.

e) Bilgisayarlarda lokal yönetici yerine kısıtlı kullanıcı ile giriş yapılıp kullanılması,
f) Windows ve Antivirüs uygulamasının güncellenmeleri,
g) Lisansı olmayan ya da zararlı uygulamalar,
ğ) Virüs taramaları,
h) Bütün PC ve dizüstü bilgisayarlar otomatik olarak en geç 15 dakika içerisinde şifreli ekran korumasına geçebilmeli,
ı) Dizüstü bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
i) Dizüstü bilgisayarın çalınması kaybolması durumunda, durum fark edildiğinde en kısa zamanda BT sorumlusuna ve İnsan Kaynaklarına haber verilmelidir.

j) Bütün cep telefonu, akıllı telefon, tablet, taşınabilir cihazlar vb. firmanın ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (kızıl ötesi, bluetooth, vs.) özellikleri aktif halde olmamalıdır ve mümkünse Antivirüs uygulamaları ile yeni nesil virüslere karşı korunmalıdır.
k) Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek duruma ve kişiye yönelik saldırılardan (örneğin elektronik bankacılık vb.) cihazın sahibi sorumludur.
l) Gerekli olduğu zamanlarda (hastalık, rapor, işten çıkma vb.) Bilgisayar, telefon, mobil cihazların vb. kullanılması zorunluluğu olduğunda güvenlik şifreleri bölüm yöneticilerine verilmelidir. İlgili personel işin başına döndüğünde kendisine zimmetli cihaz şifresini değiştirmelidir.
m) Firmanın bilgisayarlarını kullanarak taciz veya yasa dışı olaylara karışılmamalıdır.
n) Ağ güvenliğini (örnek: bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (*packet sniffing, packet spoofing, denial of service* vb.) ortadan kaldıracak eylemlere girişilmemelidir.
o) Kullanıcılar tarafından port veya ağ taraması yapılmamalıdır.
ö) Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. *DOS* saldırısı, port, ağ taraması vb. yapılmamalıdır.
p) Herhangi bir bilgi güvenliği olayını fark ettiğinde, zaman geçirmeden BT sorumlusuna haber vermelidir.
r) Firma bilgileri firma dışında üçüncü şahıslara iletilmemelidir.
s) Kullanıcıların kişisel bilgisayarları üzerine BT sorumlusunun onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
ş) Şirket içinde kullanılan USB gibi aygıtların kaybolması veya çalınması halinde bu durumun derhal BT sorumlusuna bildirilmesi gereklidir.
t) Cihaz, yazılım ve veri, izinsiz olarak kurum dışına çıkarılmamalıdır.
u) Firma kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (dergi CD'leri veya internetten indirilen programlar vb.) kurmak ve kullanmak yasaktır.
ü) Yetkisi olmayan personelin firmadaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
v) Kurumsal veya kişisel verilerin gizliliğine veya mahremiyetine özel önem gösterilmelidir. Bu veriler, firmanın bu konudaki yasal mevzuatlar saklı kalmak kaydıyla elektronik veya kâğıt ortamında üçüncü kişi ve kurumlarla paylaşılamaz.
y) Firma çalışanları, firma personeli olduğu sürece ve firmadan ayrılmaları (emeklilik, istifa vb.) durumlarında kurum bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur.
z) Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin düzenli olarak çeşitli ortamlarda (CD, DVD, USB, harici disk vb.) yedeklenmesi yasaktır.
aa) BT tarafından atanan yetkili kişiler kullanıcıya haber vermeden yerinde veya uzaktan çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel kişisel

bilgisayarlardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.

bb) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.

cc) Bilgisayarlar üzerinde firma belgeleri ve onaylı uygulamalar haricinde dosya alışverişinde bulunulmamalıdır.

çç) Binalarda sorumlu BT sorumlusunun bilgisi dışında bilgisayarlar, ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemeler değiştirilmemelidir.

dd) Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.

ee) Gerekmedikçe bilgisayar kaynaklarını paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

ff) Unutmayalım ki başta bilginin sahibi olmak üzere tüm firma çalışanları bilgi güvenliğinden sorumludur.

gg) Bu nedenle tüm çalışanların yılda bir kez yapılan Bilgi Güvenliği Farkındalık Eğitimine katılması zorunludur.