



# T.C. SAĐLIK BAKANLIĐI

## PERSONEL İÇİN BİLGİ GÜVENLİĐİ POLİTİKASI

Kurumsal Bilgi Güvenliđi Yönetim Politikası Bildirimi

Doküman Sürüm : 1.0  
Tarih : Eylül 2007



Bakanlığımız bilişim sistemlerinde çok önemli fonksiyonlar icra edilmekte olup bu bilgilerin güvenliği, gizliliği ve kişisel mahremiyetin korunması büyük önem arz etmektedir. Ağa bağlı olan herhangi bir bilgisardaki güvenlik açığı Bakanlığımızın bütün bilişim sistemlerinin güvenliğini riske atmasına sebep olabilir.

Bu nedenle Kurumsal Bilişim sistemlerinin güvenliğinde herhangi bir aksatmaya mahal verilmemesi için genel sistem seviyesinde alınmış olan güvenlik tedbirleri yanında çalışanlarımızda bu hususta titizlikle uyması gereken bir takım kurallar vardır. Bu kurallara bütün Bakanlığımız çalışanları uymak zorundadır. Uyulması gereken kurallar aşağıda belirtilmiştir.

### 1.Eposta Kullanma Kuralları

- a) Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
- b) Zincir mesajlar ve mesajlara iliştilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- c) Kişisel kullanım için İnternet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
- d) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
- e) Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- f) Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb) gönderemezler.
- g) Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
- h) Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-maillerin sahte e-mail olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- i) Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
- j) Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.
- k) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu mailler virus, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler.
- l) Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.
- m) Elektronik postaların sık sık gözden geçirilmesi, gelen mesajların uzun süreli olarak genel elektronik posta sunucusunda bırakılmaması ve bilgisayardaki kişisel klasör'a (personel folder) çekilmelidir.
- n) Sağlık Bakanlığı çalışanları gönderdikleri, aldıkları veya sakladıkları e-maillerde kişisellik aramamalıdır. Yasadışı ve hakaret edici e-posta haberleşmesi yapılması durumunda yetkili kişiler önceden haber vermeksizin e-mail mesajlarını denetleyebilir ve kullanıcı hakkında yasal ve idari işlemler başlatılabilir.
- o) Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludurlar. Şifrelerinin kırıldığını farkettiler andan itibaren yetkililerle temasa geçip durumu haber vermekle yükümlüdürler.
- p) Altı ay süre ile kullanılmayan e-posta kutuları Bilgi İşlem birimi tarafından kaldırılabilir. Kurumdan ayrılan personel kurumsal e-posta sistemini kullanamaz. Eposta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma, işten ayrılma



sebepleriyle kurumdaki değişikliğinin yetkililer tarafından Bilgi İşlem Daire Başkanlığına en kısa zamanda bildirilmesi gerekmektedir.

## 2.Şifre Kullanma Kuralları

- Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her dört ayda birdir.
- Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Şifreler başkası ile paylaşılmaması, kağıtlara yada elektronik ortamlara yazılmamalıdır.
- Şifrelemede, küçük ve büyük karakterlere (örnek, a-z, A-Z), hem dijit hemde noktalama karakterleri ve ayrıca harflere (örnek;0-9, !@#\$%^&\*()\_+|~=-\`{}[]:;'<>?,./) sahip olmalıdır.
- En az sekiz adet alfanümerik karaktere sahiptir.
- Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
- Aile isimleri kullanılmamalıdır.
- Herhangi bir kişiye telefonda şifre verilmemelidir.
- e-posta mesajlarında şifre yazılmamalıdır.
- Şifreler aile bireyleri ile paylaşılmamalıdır.
- Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.
- Bir kullanıcı adı ve şifresinin birim zamanda birden çok Bilgisayarda kullanılmamalıdır.
- Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

## 3.Anti-virus Politikası

- Bütün bilgisayarlarda kurumun lisanslı anti-virus yazılımı yüklü olmalıdır ve otomatik olarak güncellenmelidir.
- Anti-virus yazılımı yüklü olmayan bilgisayarlar ağa bağlanmamalıdır.
- Zararlı programları (örnek, virusler, solucanlar, truva atı, e-mail bombaları, vs) Kurum bünyesinde oluşturmak ve dağıtmak yasaktır.
- Hiçbir kullanıcı herhangi bir sebepten dolayı anti-virus programını sisteminden kaldıramaz.

## 4.İnternet Kullanım Politikası

- Hiçbir kullanıcı peer-to-peer bağlantı yoluyla internetteki servisleri kullanamayacaktır. (Örnek; KaZaA, iMesh, eDonkey2000, Gnutella, Napster, Aimster, Madster, FastTrack, Audiogalaxy, MFTP, eMule, Overnet, NeoModus, Direct Connect, Acquisition, BearShare, Gnucleus, GTK-Gnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, XoLoX, OpenNap, WinMX. v.b.)
- Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ,MIRC,Messenger v.b. mesajlaşma ve sohbet programları gibi chat programlarının kullanılmaması. Bu chat programları üzerinden dosya alışverişinde bulunulmaması.
- Hiçbir kullanıcı internet üzerinden Multimedia Streaming yapamayacaktır.
- Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.
- İş ile ilgili olmayan (müzik, video dosyaları ) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek yasaktır.
- İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve Kurum sistemleri üzerine bu yazılımlar kurulamaz.





- g) Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemesi ve dosya indirimi yapılmamalıdır.
- h) Bilgisayar İşletim Sistemleri için büyük ölçüde tehdit ettiği için internet üzerinden ekran koruyucu, masaüstü resimleri, yardımcı program olduğu belirtilen araçlar gibi her türlü dosya ve programların indirilmesi/kopyalanması yasaktır.
- i) Üçüncü şahısların kurum içerisinden internetini kullanmaları Bilgi İşlem sorumlusunun izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.
- j) Kurum, iş kaybının önlenmesi için çalışanların internet kullanımını hakkında gözlemlene ve istatistik yapabilir.

## 5.Genel Kullanım Politikası

- a) Bütün PC ve laptoplar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmelidir.
- b) Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
- c) Kurumda domain (çalışma alanı) yapısı varsa mutlaka login olunmalıdır. Bu durumda, domain'e bağlı olmayan bilgisayarların yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.
- d) Laptop bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi İşlem Şubesi'ne de haber verilmelidir.
- e) Bütün Cep telefonu ve PDA (Personal Digital Assistant) cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, vs) özellikleri aktif halde olmamalıdır ve mümkünse anti-virus programları ile yeni nesil virüslere karşı korunmalıdır.
- f) Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek kuruma veya kişiye yönelik saldırılardan (örnek, elektronik bankacılık vs.) sistemin sahibi sorumludur.
- g) Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.
- h) Ağ güvenliğini (örnek, bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (paket sniffing, paket spoofing, denial of service vs. ). Ortadan kaldıracak eylemlere girişmemelidir.
- i) Port veya ağ taraması yapılmamalıdır.
- j) Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.
- k) Kurum bilgilerini kurum dışından üçüncü şahıslara iletilmemelidir.
- l) Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Şubesinin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
- m) Cihaz, yazılım ve verinin izinsiz olarak kurum dışına çıkarılmamalıdır.
- n) Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD'leri veya internetten indirilen programlar vs) kurmak ve kullanmak yasaktır.
- o) Yetkisi olmayan personelin, Kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
- p) Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, Bakanlığımızın bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilemez.
- q) Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin düzenli olarak farklı ortamlara ( cd, dvd, usb, external harddisk vs..) yedeklenmesinden sorumludur.





- r) Bilgi İşlem birimi 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 bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.
- s) Bilgisayarlarda oyun ve eğlence amaçlı programların çalıştırılmamalı/ kopyalanmamalıdır.
- t) Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
- u) Kurumda Bilgi İşlem biriminin bilgisi olmadan Bakanlık Ağ sisteminde (web hosting servisi, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.
- v) Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları ,kaynak profilleri v.b. üzerinde mevcut yapılan düzenlemelerin hiçbir surette değiştirilmemelidir.
- w) Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.
- x) Gerekmedikçe bilgisayar kaynaklarını paylaşımına açılmamalıdır, kaynakların paylaşımına açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.