ERİŞİM DENETİMİ POLİTİKASI

Güncelleme Sayısı: 00 Güncelleme Tarihi:

a. STB giriş sisteminde bulunan kart okuma cihazına her personel için tanımlanma yapılmıştır. Personel ayrıca yaka kartını kullanır.

b. Borsa içerisinde kullanılan ana makinedeki İşletim Sisteminde tüm bilgisayarların kullanıcı tanımlarının ve erişim yetkilerinin belirlendiği aktif dizin oluşturulmuştur.

c. Aktif dizine bağlanan kullanıcı parolaları bilgi teknolojileri kullanıcı sözleşmelerinde yer aldığı gibi belirlenir.

d. Her personel kullanıcı şifresi ile sisteme girebilmektedir. Yetkilendirme sadece üst yönetim tarafından yapılmaktadır.

e. Erişim gereksinimi artık kalmamış kullanıcılar için birim amiri tarafından bilgi işlem bilgilendirilir ve ona göre hareket edilir. Sistemden de bu personelin erişim şifresi silinir.

E-Posta 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 iliştirilmiş 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. Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları

cevaplandırmalıdır.

i. Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.

j. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodlar içerebilirler.

l. Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalıdır.

Anti virüs Kullanım Kuralları

a. Bütün bilgisayarda kurumun lisanslı anti virüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.

b. Anti virüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem Sorumlusuna haber verilmelidir.

c. Zararlı programları (örneğin, virüsler, solucanlar, truva atı, e-mail bombaları vb) kurum bünyesinde oluşturmak ve dağıtmak yasaktır.

d. Hiçbir kullanıcı herhangi bir sebepten dolayı anti virüs programını sistemden kaldıramaz ve başka bir anti virüs yazılımını sisteme kuramaz.

İnternet Kullanım Kuralları

a-Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.

b. İş ile ilgili olmayan yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek yasaktır.

c. İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz.

d. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.

e. Bilgisayar işletim sistemlerine zarar verdiği için internet üzerinden ekran koruyucu, yamalar, masaüstü resimleri, yardımcı, tamir edici program olduğu belirtilen araçlar gibi her türlü dosya ve programların indirilmesi ve/veya kurulması yasaktır.

Genel Kullanım Kuralları

a-Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.

b. 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.

c. Laptop bilgisayarın çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Birimi' ne haber verilmelidir.

d. Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) sistemin sahibi sorumludur.

e. Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.

f. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak eylemlere girişmemelidir.

g. Port veya ağ taraması yapılmamalıdır.

h. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DOS saldırısı, port-network taraması

vb. yapılmamalıdır.

ı. Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.

i. Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.

j. Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD' leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.

k. Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.

l. Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin düzenli olarak farklı ortamlara (cd,dvd, usb, External Harddisk vb) yedeklenmesinden sorumludur.

m. Bilgi İşlem sorumlusu kullanıcıya haber vermeksizin 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.

n. Birimlerde Bilgi İşlem sorumlusu dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.

o. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.

ö. Bilgisayar üzerinde bir problem oluştuğunda, ivedilikle Bilgi İşlem Sorumlusuna haber verilmelidir.

GENEL SEKRETER	YÖNETİM KURULU BAŞKANI
Yasemin ARIKAN	Cevdet METE