**18.5. Genel Kullanım Politikası**

**18.5.1.** Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir.

**18.5.2.** Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.

**18.5.3.** Kurumda domain (çalışma alanı) yapısı varsa mutlaka login (oturum açılmalıdır) olunmalıdır. Bu durumda, domain’e bağlı olmayan bilgisayarlar yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.

**18.5.4.** Laptop bilgisayarın çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Birimine haber verilmelidir.

**18.5.5.** Bütün kullanıcılar kendi bilgisayarlarının güvenliğinden sorumludur. Açık bırakılması halinde veya kullanıcı oturum şifrelerinin ikinci şahıslarca biliniyor olması durumlarında bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) bilgisayarın sahibi sorumludur.

**18.5.6.** Kurumun bilgisayarları kullanılarak taciz veya yasadışı olaylara karışılmamalıdır.

**18.5.7.** Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packetsniffing, packetspoofing, denial of service vb.) eylemlere girişilmemelidir.

**18.5.8.** Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DOS saldırısı, port network taraması vb. yapılmamalıdır.

**18.5.9.** Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.

**18.5.10.**Cihazlar, yazılımlar ve veriler izinsiz olarak kurum dışına çıkarılmamalıdır.

**18.5.11.** Port veya ağ taraması yapılmamalıdır.

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

**18.5.13.** Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.

**18.5.14.** Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programlar (Dergi CD’leri veya internetten indirilen programlar vs.) kurulmamalı ve kullanılmamalıdır.

**18.5.15.** Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, Kurumumuzun bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kâğıt ortamında üçüncü kişi ve kurumlara verilemez.

**18.5.16.** Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin güvenliği ile sorumludur.

**18.5.17.** Bilgi İşlem Birimi tarafından yetkili kişiler kullanıcıya haber vermek kaydı ile yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel bağlanılan bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.

**18.5.18.** Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.

 **18.5.19.** Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

**18.5.20.** Kurumda Bilgi İşlem Biriminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.

**18.5.21.** Birimlerde sorumlu Bilgi İşlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarlarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.

**18.5.22.** Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Lisansız yazılımı bilgisayarında barındıran personel ilgili mevzuat çerçevesinde kendisi sorumludur.

**18.5.23.** Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

**18.5.24.** Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir.