

**T.C.**

**ÇUKUROVA KALKINMA AJANSI**

**BİLGİ GÜVENLİĞİ POLİTİKASI**

**T.C.** **ÇUKUROVA KALKINMA AJANSI**

**BİLGİ GÜVENLİĞİ POLİTİKASI USUL VE ESASLARI**

**BİRİNCİ BÖLÜM GENEL HÜKÜMLER**

**Dayanak**

**(1)** Bu usul ve esaslar, 5449 sayılı Kalkınma Ajanslarının Kuruluşu Koordinasyonu Ve Görevleri Hakkında Kanun ve 2009/15433 sayılı Bakanlar Kurulu kararına ekli Kalkınma Ajansları Çalışma Usul ve Esasları ve ilgili diğer mevzuat hükümleri çerçevesinde hazırlanmıştır.

**Amaç ve Kapsam**

**(2)** Bu usul ve esasların amacı; T.C. Çukurova Kalkınma Ajansı bünyesinde kullanılan ağ (network) altyapısı, internet altyapısı, bilgisayarlar ile bunlarla bütünleşen bilişim kaynaklarının (yazılım, donanım) kullanımına ilişkin ilkeleri belirlemektir.

**(3)** Bu usul ve esaslar; T.C. Çukurova Kalkınma Ajansı bilişim hizmetlerinden yararlananların, bu hizmetlerin etkin ve verimli kullanımı için uyması gereken kuralları kapsar.

**Tanımlar**

**(4)** Bilgi güvenliği politikası usul ve esaslarında geçen;

a) Ajans: T.C. Çukurova Kalkınma Ajansını,

b) Bilgisayar Ağı: Hizmet binasındaki bilgisayarlar arası bilgi ve veri iletişiminin yapılabildiği ve paylaşılabildiği bilgi sistemlerinin meydana getirdiği bilgisayar donanımı, yazılımı ve yan birimlerinden meydana gelen yapıyı,

c) Bilgi İşlem Kaynakları: Hizmet sunucu bilgisayarlar, kişisel bilgisayarlar, yazıcılar, faks ve modem cihazları, compact disk okuyucuları ve kayıt edicileri (CD ve DVD gibi), teyp backup üniteleri, tarayıcılar (scanner), disk (hard disk) birimleri, disket sürücüleri ve benzerleri gibi elle tutulan ve gözle görülebilen unsurları,

ç) Dışarıdan Erişim: Ağ kaynaklarına ve erişilmek istenilen bilgiye fiziksel olarak farklı bir ağda bulunan bilgisayar aracılığı ile erişim sürecini,

d) Dosya: Herhangi bir kayıt ortamında saklanan kayıtlar topluluğunu,

e) Güvenlik Duvarı (Firewall): Yetkisiz erişimi ve her türlü saldırıyı engellemek amacıyla, güvenilir bir ağ ile herkese açık bir ağ arasına yerleştirilen güvenlik programını,

f) Güvenlik İhlali: Bilgi güvenlik politikası ve talimatlarını ihlal eden veya bununla ters düşen herhangi bir olayı,

g) Hizmet Sunucu Bilgisayar (Server): Kendisine bağlanan kullanıcılara belli hizmet ve fonksiyonları sağlayan gelişmiş bilgisayarları,

ğ) Hassas Bilgi: Açığa çıkması halinde, ilgili kişi ve kuruluşlara ciddi zararlar verebilecek verileri,

h) İnternet: Dünya çapında belli bir protokolü (TCP/IP) kullanarak, bilgisayarlar arasında haberleşme ve bilgi paylaşımını sağlayan iletişim ağını,

ı) İndirme (Download): İnternetten veya herhangi bir uygulamadan yapılan bilgi transferini,

i) İletişim: Bir bilgisayar ortamındaki bilgi ve verinin, veri iletişim ortam ve yöntemlerini kullanarak başka bilgisayar ortamlarına aktarılmasını,

j) İşletim Sistemi (Operating System): Bilgi işlem kaynaklarının yönetilmesini sağlayan yazılım sistemlerini,

k) Kişisel Bilgisayar (PC): Tek kullanıcılı, içinde bir mikro işlemci olan bilgisayarları,

l) Modem: Telefon hatları, kablolar veya mikrodalga gibi transmisyon ortamları üzerinden iletebilecek duruma getirmek üzere verileri kodlayan aygıtı,

m) Oturum (Session): Bir kullanıcının, kullanıcı kodunu ve parolasını bilgisayara girmesinden, işini bitirip bilgisayarla bağlantısını kesmesine kadar yaptığı çalışmanın genel adını,

n) Protokol (IP): Bilgisayarların internet üzerinden nasıl iletişim kuracağını belirleyen kurallar setini,

o) Parola-Şifre (Password): Verilere ve bilgisayar sistemine yetkisiz erişimi önlemek için tanımlanmış kod veya karakterleri,

ö) Router: Ağlar arasındaki bağlantıları gerçekleştiren cihazları,

p) Sistem Yöneticisi (System Administrator): Bilgi işlemden sorumlu destek personeli

r) Şifreleme: Bilgiyi gizli bir şifre veya anahtar olmadan okunamayacak (deşifre edilemeyecek) bir kod haline getirme işlemini,

s) Uç Kullanıcı: Bilgisayar ağı kullanıcılarını,

ş) Virüs: Bilgisayarlara değişik yollarla girebilen ve bu bilgisayar programlarının yapması gereken asıl fonksiyonlarını hiç yaptırmayan, kısıtlayan veya yanlış işlemler yaptıran yazılım ve programları,

t) Veri: Üzerinde işlem yapılmak üzere bilgisayar ortamına aktarılan ham bilgiyi,

u) Veri Tabanı Yönetim Sistemi: Üretilen bilgilerin yapısal formlarda tutulduğu ve birbirleriyle olan ilişkilerin sağlandığı yazılım sistemlerini,

ü) Yetki: Kullanıcıların bir bilgisayar sistemindeki çevre birimlere ve depolanmış verilere erişebilmesi veya sisteme girebilmesi için verilmiş olan izni,

v) Yazılım: Bir bilgisayar sisteminde çalışmak üzere tasarlanmış bir uygulamayla ilgili kod, prosedür ve ilişkili dokümandan oluşan yapıyı,

y) Web Tarayıcı (Browser): İnternet sayfalarını görüntülemek için kullanılan programı, ifade eder.

z) Bilişim Komisyonu: Bilgi işlem destek personeli ve Genel Sekreterin görevlendireceği 3 ajans personeli

 ifade eder.

**İKİNCİ BÖLÜM**

**BİLGİ İŞLEM KAYNAKLARI VE PROGRAMLARININ ALIM, KURULUM, YAZILIM,**

**BAKIM, ONARIM, EĞİTİM SEMİNERLERİ VE PROGRAM TEMİNİ**

**(5)** Ajans, bilgi işlem kaynakları ile programlarının alımı, kurulumu, bakımı ve onarımı konularında aşağıdaki usul ve esaslar uygulanır;

a) Cari yıl için konulan ödenek nispetinde alımların gerçekleştirilebilmesi için, birimler; yıllık bilgi işlem kaynakları ve bilgisayar programlarına ilişkin öngörülebilen taleplerini bilgi işlemden sorumlu personelin bağlı olduğu birime bildirirler.

b) Bilişim komisyonu; alınacak malzemenin mevcut sisteme uyumluluğu veya parçanın sisteme eklemlenebilirliği açısından hizmet gereklerini ve yıllık bütçe imkânlarını dikkate alarak, birimlerden gelen bu teklifleri değerlendirip karara bağlar. Bu konuda alınan kararlar, bir tutanakla Genel Sekreterin oluruna sunulur.

c) Alınmasına karar verilen bilgi işlem kaynakları ile ilgili teknik şartnameler; alınacak sistemlerin günün teknolojisine uygunluğu düşünülerek bilişim komisyonu tarafından hazırlanır.

ç) Birimlerin ihtiyacı olan bilgi işlem kaynaklarının alımının gerçekleştirilmesi için bilişim komisyonu kararı ve hazırlanan teknik şartname, Genel Sekreterlik tarafından görevlendirilen satın alma komisyonuna intikal ettirilir.

d) Bilgi işlem kaynakları ile programlarının bakım ve onarım işlemleri sarf malzeme takip işlemleri, bilgi işlemden sorumlu personelin bağlı olduğu birim tarafından yapılır ya da yaptırılır.

e) Satın alınan bilgisayar ve malzemelerinin program veya sürücü CD’leri ile lisansları, gerektiğinde kullanılmak üzere bilgi işlemden sorumlu destek personel tarafından arşiv ve muhafaza edilmesi sağlanır.

(f) Bilgisayar programlarına ilgisiz ve yetkisiz kişilerce müdahale edilemez. Bilgisayar programlarıyla ilgili güncellemeler ve değişiklikler, bilgi işlemden sorumlu personel tarafından veya Genel Sekreter tarafından görevlendirilmek kaydıyla diğer personel tarafından ve bilgi işlemden sorumlu personel gözetiminde yapılır.

(g) Birimler; kendi hizmet ve faaliyetleriyle ilgili programları, hangi personelin kullanacağını ve yetki sınırlarını bilgi işlem hizmetlerinden sorumlu birime bildirirler ve bu teklifler doğrultusunda, programlara girişlerle ilgili teknik yetkilendirme ve yönlendirmeler, bilgi işlemden sorumlu destek personel tarafından yapılır.

**ÜÇÜNCÜ BÖLÜM**

**BİLGİSAYARLAR, VERİ VE BİLGİ GÜVENLİĞİ TEDBİRLERİ**

**Fiziksel Güvenlik**

**(6)** Hizmet binalarında, bilgi işlem kaynaklarının güvenliği için, aşağıda belirtilen fiziksel tedbirler alınır:

a) Sistem odalarının yakınında yangın söndürme cihazları bulundurulur. Cihazlarda kullanılacak kimyasal maddelerin seçiminde ise, bilgisayarlara zarar vermeyecek olanlar tercih edilir.

b) Sistemin meteorolojik etkilerden korunması amacı ile sistem odalarını 20- 25 C arası sıcaklıkta tutacak havalandırma tertibatı kurulur.

c) Sabit olmayan depolama üniteleri kullanılmadıkları zamanlarda, bilgisayarların üzerinde bırakılmaz ve basılmış dokümanların yanı sıra bu üniteler de uygun kilitli ortamlarda korunur.

ç) Toprak hattı, sigortalama ve kesintisiz güç kaynağı ile sistemin korunması sağlanır.

d) Bilgi işlem personeli, bu işle görevlendirilmiş diğer Ajans personeli ya da dışarıdan temin edilen bilgi işlem desteğiyle sorumlu teknik uzmanlar haricinde hiç kimse bilgisayarların iç kısmını açamaz.

**Veri ve Bilgi Güvenliği**

**(7)** Ajans bilgi sistemlerinde güvenliğin sağlanmasına yönelik olarak aşağıda belirtilen ilke ve kurallar uygulanır:

a) Bilgi işlem hizmetlerinden sorumlu birim tarafından, her uç kullanıcının bilgisayarına, kullanıcının ismi ile parolası verilir ve tanıtılır. Tüm uç kullanıcılar; kendilerine verilen bu kullanıcı adı ve parola ile bilgisayar ağına girebilir.
b) Ajans personeli olmayan kişilere kullanıcı adı ve şifre tahsis edilebilmesi için, Destek Hizmetleri Birimine yazılı talepte bulunulur ve bu talebin uygun görülmesine istinaden, bu kişiler, kendilerine verilecek geçici kullanıcı adını ve şifresini kullanırlar. Bilgi işlem hizmetlerinden sorumlu birim tarafından kendilerine kullanıcı adı ve şifresi tahsis edilmiş olanlar dışındakiler, ajansın herhangi bir biriminde mevcut bilgisayarı veya ağ bağlantı ucunu kullanamaz ve bu tür girişimlere ajans çalışanlarınca müsaade edilemez.

ç) Uç kullanıcı adıyla yapılan iş ve işlemlerdeki tüm sorumluluk, kullanıcıya ait olacaktır. Bu nedenle, hiçbir kullanıcı, kullanıcı adını ve şifresini başkaları ile paylaşamaz. Uç kullanıcı tarafından çalışmaya geçici olarak ara verdiği durumlarda, bilgisayarın başkası tarafından kullanılmaması için gereken tedbirleri alır, resmî hizmete ait CD, yığın bellek gibi bilgi depolama aygıtlarını bilgisayarından çıkararak emniyetli bir yerde muhafaza eder.

d) Bilgi işlem hizmetlerinden sorumlu birim tarafından donanım, yazılım, kısıtlama ve yönlendirme yöntemleriyle her uç kullanıcının, bilgisayar ağında var olan bilgi kategorilerinden, yalnızca kendi konusuyla ilgili alana ulaşabilmesi sağlanır.

e) Kullanıcıların herhangi bir nedenle görev yerlerinin, görev ve yetkilerinin değişmesi halinde, bilgi işlemden sorumlu personeli ivedilikle bilgilendirir. Bu bildirimle birlikte, ilgilinin kullanıcı adı ve sistem parolaları, Bilgi İşlem Birimince değiştirilir.

f) Ajans bilgi sistemleri güvenliğini sağlamak amacıyla, bilgi işlem hizmetlerinden sorumlu birim tarafından kullanıcılara tahsis edilen/edilecek masaüstü veya dizüstü bilgisayarlara web tarayıcı (browser), güvenlik duvarı (firewall) ve virüs tarama (anti-virüs) gibi güvenlikle ilgili programlar yüklenir. Gerektiğinde bu programlarda özel ayarlar ve güncellemeler yapılır ve sınırlı bir kullanıcı hesabı (user account) tanımlanır. Bu programların ayarları ve kullanıcı hesabı türü, kullanıcılar tarafından kesinlikle değiştirilemez. Bu konuda gerekli değişikliklerin yapılmasından Sistem Yöneticisi sorumludur.

g) İçerisinde yüksek gizlilik dereceli bilgiler bulunan bilgisayarlar, ajans bilgisayar ağına bağlanamaz, bilgisayar ağına bağlanmış olan bilgisayarlara yüksek gizlilik dereceli bilgiler yüklenemez. Bu konudaki sorumluluk, bilgisayar kullanıcılarına aittir.

ğ) Ana makinelere, yedekleme üniteleri tarafından otomatik olarak yedekleme yapılır. Yedeklenen bilgilerin bulunduğu CD, yığın bellek vb. üniteler güvenli yerlerde korunur.

h) Bilgi sistemleri üzerinde güvenlik araştırması yapmak için yetkilendirilmemiş hiçbir personel bu araştırmaları yapamaz ve güvenlik mekanizmalarını test etme girişiminde bulunamaz. Güvenlik mekanizmalarının bozulmasına neden olabilecek her türlü eylem ve işlem yasaktır.

ı) Kullanıcılar, kendilerine tahsis edilen/edilecek olan bilgisayar veya diğer malzemenin amaç dışı kullanılmasından dolayı cezai ve disiplin yönlerinden sorumludurlar.

i) Kullanıcılar, ajans bilgi sistemindeki bilgileri, izinsiz olarak iletişim araçları ve internet vasıtasıyla veya diğer herhangi bir biçim ve yöntemle yayınlayamaz ve açıklayamazlar.

j) Kullanılan güvenlik ürünlerinin işlerliği, bilişim komisyonu tarafından düzenli testler ve otomatik izleme/uyarı sistemleri ile takip edilir. İzleme sonucunda alınan raporların bir kopyası, sistem üzerinde güvenlik ihlaline yol açan bir durum ortaya çıktığında delil olarak kullanılmak üzere bilgi işlemden sorumlu personel tarafından saklanır.

k) Ajans personeli, ajans bilgi sistemleri güvenliğinin sağlanmasına yönelik olarak yukarıda belirtilen ilke ve kurallara riayet etmek zorundadır.

**DÖRDÜNCÜ BÖLÜM**

**İNTERNET, WEB SİTESİ VE E -POSTA HİZMETLERİ**

**Bilgisayarların İnternet Ortamına Açılması**

**(8)** Ajans bilgisayarlarının internet ortamına açılması ile ilgili usul ve esaslar şunlardır:

a) Ajansta internet ortamına açılacak bilgisayarlar; bilişim komisyonunca yapılacak güvenlik ve teknik altyapı kapasitesi değerlendirilerek tespit edilir.

b) İnternet erişimi için ajans ağı kullanılmalıdır. Modem kullanarak telefon hatları vasıtası ile internet bağlantısı kurulamaz. Zorunlu hallerde Genel Sekreterin uygun görüşü ile modem kullanılarak internet bağlantısı sağlanabilir. Ancak, bu durumda modem ile internete bağlanacak bilgisayarların, Ajans bilgi sistemlerine bağlantısı yapılamaz.

**İnternet Hizmetlerinde Güvenlik**

**(9)** Ajans internet hizmetleriyle ilgili alınacak tedbirler ve riayet edilmesi gereken hususlar şunlardır:

a) Ajans internet çıkışı tek bir merkezden sağlanır. Ajans sunucu ve kullanıcı internet erişim ağını koruyan “Güvenlik Duvarı”, ağlar arasındaki veri paketlerini şifrelendirerek yönlendiren “Router”, Ajans internet güvenliği politikası uyarınca kullanıcıların internette gezebilecekleri web sitelerini filtrelemekte kullanılan “İçerik Denetleme Yazılımı”, virüslerden korunmak için kullanılan “Anti-virüs Sistemi” yönetimi, bilgi işlem hizmetlerinden sorumlu birim tarafından yürütülür.

b) Ajans bilgi sistemleri güvenliğinin sağlanması amacıyla, Genel Sekreter tarafından internet üzerindeki erişim hakları veya program kullanımları kısıtlanabilir. Bilişim Komisyonu tarafından yapılacak güvenlik değerlendirmesi sonucunda, uygun görüş ile güvenlik nedeniyle erişimi kısıtlanan veya engellenen uç kullanıcıların bilgisayarlarına konan bu engelleme ve kısıtlamalar kaldırılabilir.

c) Potansiyel olarak virüs, solucan veya bunlara benzer güvenlik açısından tehlikeli programların bulaşması/bulaştırılması tehlikesi taşıyan internet sitelerine (Yetişkin-adult-, kumar, oyun, şifre çözme-crack, saldırı-hack, illegal arama -underground search, sohbet odaları, ilgili mevzuata aykırı ve yasa dışı siteler vb.) girilmesi ve lisanssız programların internetten indirilmesi kesinlikle yasaktır.

**Web Sitesi Kurma Ve Bilgi Yayınlama**

**(10)** Ajans web sitesi oluşturma ve bu sitelerde bilgi yayınlama ile ilgili usul ve esaslar şunlardır:

a) Ajans Web Sitesi’nin tasarlanmasından ya da bu işin yaptırılmasından bilgi işlem hizmetlerinden sorumlu birim sorumludur. Sitede yer alması istenilen bilgi ve belgelerin yüklenmesi, bilgi işlemden sorumlu personel ya da yüklemenin özelliğine göre Genel Sekreter tarafından görevlendirilecek diğer personel tarafından yapılır.

**E-Posta Hesabı Açılması, Kullanılması ve Personelin Sorumlulukları**

**(11)** E-posta hesabı açılması ve kullanılmasına ilişkin iş ve işlemler ile bu konudaki sorumluluklar şunlardır:

a) Ajans resmî e-posta adreslerinin açılması, e-posta standartlarının oluşturulması ve kullanıcıların hizmetine sunulması işlemleri bilgi işlem hizmetlerinden sorumlu birim tarafından yürütülür.

b) Adına e-posta hesabı açılanların sorumluluğu, hesabın açılmasından itibaren başlar ve hesap kapatılması bildirilinceye kadar devam eder. Bu nedenle, Ajanstan ayrılan personele e-posta hesabı kapatılmadan önce bir ay süre verilir. Bir ayın sonunda hesap kapatılır.

c) E-posta hesabını 90 gün boyunca kontrol etmek amacıyla dahi kullanmayanların hesapları herhangi bir ikaz yapılmaksızın kapatılır.

ç) Göndereni belli olmayan, tanınmayan ve bu şekilde şüpheli olan ve ilgili olmadığı düşünülen e-postalar açılmadan ve ekli dosyaları çalıştırılmadan bilgisayardan silinir.

d) Islak imzalı olarak kayıt altına alınması gereken önemli durumlar dışında, personel arasındaki yazılı iletişim resmi e-posta sistemi kullanılarak sağlanır. Tüm personel, kullanımına tahsis edilen bilgisayarlar ve telefonlara e-posta hesaplarını kurar.

e) E-postalar işlerin aksamaması ve duyurulardan zamanında haberdar olunması için düzenli olarak kontrol edilir.

f) Personel özel yazışmalarında resmi e-posta adreslerini kullanamaz.

g) Birimler arasında yapılan yazışmalarda yazışmayı yapan personelin birim başkanına, kurum dışı yapılan yazışmalarda ise Genel Sekretere bilgi gönderilir.

**T.C.** **ÇUKUROVA KALKINMA AJANSI**

**BİLGİ TEKNOLOJİLERİ KULLANIMI SÖZLEŞMESİ**

**Ekipman ve Araçların Kullanımı**

1. Ajans ekipman ve sistemleri iş amaçlı kullanılmalıdır. Haberleşme araçları ve bilgi sistemlerinin kullanımında bu dokümanda ve bilgi güvenliği politikası usul ve esaslarında belirtilen kurallar tüm Ajans çalışanları tarafından uygulanmalıdır.
2. Bilgi sistemleri kaynakları iş süreçlerinin kapsamı dışında kullanılmaz, bununla birlikte, kişisel bilgisayarlarda bulunan sabit disklerde kullanıcılar özel bilgilerini tutabilirler. Ancak kişisel bilgilerin silinmesi, değiştirilmesi veya incelenmesinden Ajans sorumlu tutulamaz.
3. Çalışanlar, kullandıkları ekipmanların zarar görmesini engellemek amacıyla, düzenli ve temiz tutmakla sorumludurlar.
4. İçlerinde Ajans ile ilgili hassas bilgilerin yer aldığı dizüstü bilgisayar veya diğer taşınabilir bilgisayar sahipleri, bu bilgisayarları hiçbir zaman, başkalarının kolayca erişebileceği yerlerde, korumasız bırakmamalıdır.
5. Kullanıcı kişisel bilgisayarının başında olmadığı sürece, bilgisayarını kapatmalı veya bilgisayarını kilitlemelidir.
6. Kullanıcı, Ajans’ta başka bir kullanıcının kişisel bilgisayarının korumasız olarak (lock edilmemiş veya şifreli ekran koruyucu olmayan) bırakıldığını gördüğünde, derhal kişisel bilgisayarın sahibine ve/veya bu kullanıcının bağlı olduğu birim başkanına durumu bildirerek gerekli önlemin alınması konusunda uyarıda bulunmalıdır.
7. Kullanıcılar, başka kullanıcılara tahsis edilmiş kişisel bilgisayarlar üzerinden zaruri durumlarda ancak bilgisayar sahibinden veya yöneticisinden izin almak suretiyle ve sisteme kendi kullanıcı adı ve şifresiyle giriş yaparak erişebilir.
8. Kullanıcının bilgi sistemlerinde bulunan bir kaynağa erişebiliyor olması, bu kaynak üzerinde kullanım hakkı, izni veya yetkisi olduğu anlamına gelmez. Kullanıcı, bilgi sistemlerinde bulunan bir kaynağa kullanım hakkı, izni veya yetkisi olmadığı halde erişebiliyor olabilir ve böyle bir durum kullanıcı tarafından derhal Bilgi İşlem Sorumlusuna bildirilmeli, kaynak kesinlikle kullanılmamalıdır.
9. Kullanıcı, diğer kullanıcıların sistem kullanımını engellemek, sistem performansını düşürmek, izinli olmadığı kaynaklara erişmeye çalışmak, bu kaynaklar için yetki almak, fazladan kaynak erişimi sağlamak ve bilgi sistemleri güvenliğini atlatmak gibi Ajans etik kurallarına ters düşen maksatlarla hareket etmemelidir.
10. Kullanıcılar kişisel bilgisayarlarına iş süreçlerini kolaylaştıracak, mesleki ve bireysel gelişimlerini sağlayacak yazılımlar kurabileceklerdir. Kişisel bilgisayara yazılım kurulumu öncesinde kullanıcı yazılımın güvenilir bir kaynaktan geldiğini, lisans ve telif hakkı ihlali olmadığını doğrulamalıdır veya bu konuda Bilgi İşlem Sorumlusuna başvurmalıdır. Herhangi bir telif hakkı ihlalinde programı yükleyen kişi bizzat sorumlu olacaktır.
11. Kullanıcılar, bilgisayar ve iletişim sistemlerinin güvenliklerini test etmek amaçlı, onaysız sistem kırma (hacking), şifre kırma (tahmin etme), dosya deşifreleme, yasadışı yazılım kopyalama veya benzer bir şekilde güvenliği zedeleyici yetkisiz işlemler yapmamalı ve yapmaya teşebbüs etmemelidir.
12. Kullanıcı özel olarak yetkilendirilmediyse, bilgi sistemlerinde bulunan hiçbir kaynağın (donanımın, yazılımın- herhangi bir program veya işletim sistemiyle ilgili sistem ayarları, uygulama yazılımı ayarları vb.) konfigürasyonunu ve ilgili ayarlarını değiştirmemelidir. Bu gibi ihtiyaçlarını Bilgi İşlem Sorumlusuna iletmelidir.
13. Kullanıcı kullandığı bilgi sistemleri üzerinde kendi denetiminde olan bir bilgiyi (dosya, klasör vb.) paylaşıma açacaksa, bu işlemin yetkisi olmayan diğer kullanıcılara hak tanımamasını sağlamalıdır. Gerekiyorsa işlemi gerçekleştirmeden önce teknik destek almalıdır.
14. Kişisel bilgisayarlar üzerine, lisansı olmadan herhangi bir program kurulmamalı ve kullanılmamalıdır.
15. Kullanıcılar bilgi sistemlerinde herhangi bir şekilde hassas bilginin silinmesi, kaybolması, üçüncü şahıslara izinsiz gösterimi veya bu durumlardan şüphe duyulması halinde hemen bağlı oldukları yöneticisine ve Bilgi İşlem Sorumlusuna durumu raporlamalıdır.
16. Kullanıcılar fax, fotokopi makinaları, masaüstü telefonlar, ajans tarafından tahsis edilen Blackberry telefonlar, kağıt öğütme cihazı, parmak izi cihazı, kameralar ve kuruma ait olan diğer tüm cihaz ve ekipmanları azami dikkatle kullanmalıdır. Herhangi bir arıza durumunda kendisi müdahale etmeden Bilgi İşlem Sorumlusuna başvurmakla sorumludur.
17. Kurum bünyesinde elektrik kesintileri için bir güç kaynağı bulunmaktadır. Elektrik kesintisi olduğunda kullanıcılar derhal açık olan belgelerini kaydedip bilgisayarlarını kapatmakla sorumludurlar.

**Kullanıcı Kodu/Şifre Kullanımı**

1. Ajans bilgi sistemleri kullanıcıları; erişme ve kullanmaya yetkili oldukları, kişisel bilgisayarlarına, uygulamalara(e-posta, aktif dizin, v.b.) ve sistem yazılımlarına kendi kullanıcı kodları ve şifreleri ile girmelidir.
2. Kullanıcılar, kullanıcı kodlarını ve şifrelerini korumakla yükümlüdür.
3. Kullanıcılar kendilerine ait kullanıcı kodu ve şifresini üçüncü şahıslara vermemelidir. Kullanıcının şifresini üçüncü şahıslara vermesinden kullanıcının kendisi sorumludur.
4. Kullanıcılar; kendi kod ve şifrelerinin bilgileri dışında kullanılması, ya da kullanıcı kod ve şifrelerinin başkası tarafından ısrarla istenmesi gibi, ağ güvenliğini tehlikeye atacak şüpheli durumları, derhal Bilgi İşlem Sorumlusuna bildirecektir.
5. Kullanıcının bilgisayara giriş, e-posta uygulamaları kullanmak için tanımlı kullanıcı adının şifresinin unutulması vb. durumlarda Bilgi İşlem Sorumlusuna bildirimde bulunulmalıdır. Kullanıcılar, tahmin edilmesi ve bulunması zor olan, kullanıcı hakkında bilgileri içermeyen şifreler seçmelidir. Şifreler paylaşılmayacak veya otomatik sistem girişleri sırasında kaydedilmeyecektir.
6. Şifreler güvenli bir ortamda saklanacaktır. Tüm kullanıcı kodları ve şifreleri asla yazılı tutulmayacak ya da e-posta ile gönderilmeyecektir. Şifrelerin yazılı tutulması, kolay şifrelerin seçilmesi şifrelerin ele geçmesine yol açabileceği için tercih edilmeyecektir.
7. Şifreler, bilgisayar sistemi üzerine asla korunmasız biçimde depolanmayacaktır.
8. Kullanıcı, şifresini ilk girişte ve ömrü bittikçe veya sistem ya da şifrenin güvenliğinin tehlikeye düştüğü durumlar ortaya çıktığı zaman değiştirmelidir.
9. Donanım ve yazılım üreticileri tarafından verilmiş olan ilk şifreler, derhal değiştirilmeli ya da ihtiyaç duyulmadığı an iptal edilmelidir.

**İnternet Kullanımı**

1. Kullanıcılar Internet’i, iş süreçlerini etkileyecek teknolojik ve hukuksal bilgilerden anında haberdar olmak ve paydaşlara (Proje Sahipleri, Yerel Aktörler, Ortak çalışma yürütülen kuruluşlar v.b.) erişerek kendi tanıtımını yapmak amacıyla kullanacaktır. Bu kapsamda kullanıcılara web filtreleri sayesinde erişim yetkisi tanınacaktır. Bu yetkiler düzenli aralıklarla ve ihtiyaç duyulduğunda düzenlenecektir.
2. Ajans, personelinin kişisel gelişimine katkıda bulunmak amacıyla, Internet kullanımını teşvik eder, ancak, kişisel gelişimi arttırıcı araştırma ve geliştirme faaliyetleri iş zamanında değil, kişisel zamanlarda, maliyetler ve iş süreçleri de göz önüne alınarak yapılacaktır.
3. İnternet kullanımındaki esas, kullanıcıların Ajans içi görev ve sorumluluklarını yerine getirirken Internet’i kullanmalarıdır.
4. Kullanıcıların Ajans’ta zamanlarını ve kaynaklarını kişisel kazanç için kullanmaları yasaktır.
5. İnternet ortamının sağladığı olanaklar, yasa dışı biçimde, insanlara zarar verme, başkalarının işlerini engelleme, gizli ve kişisel bilgilerini ele geçirip yararlanma, her türlü sahtekarlık, yolsuzluk, dolandırıcılık ya da hırsızlık gibi kötü amaçlı kullanılmayacaktır.
6. İletişim sistemlerini kullanarak, web filtresini değişik yöntemlerle aşmaya çalışarak yönetimce yasaklanmış olan adreslere girmek, materyallere ulaşmak ve bunları dağıtmak yasaktır.
7. İnternet vasıtasıyla, telif hakkı bulunan yazılımların ve diğer elektronik ürünlerin(müzik, film, e-kitap v.b.) yetkisiz bir şekilde indirilmesi, çoğaltılması ve dağıtılması yasaktır.
8. Kullanıcılar, Internet’te Kurum kimliklerini göz önüne alarak hiçbir şekilde Kurum kimliğini zedeleyici herhangi bir girişimde bulunmayacaktır. Hiçbir şekilde Internet’te Ajansa ait hassas bilgiler açıklanmayacaktır.
9. Ajans çalışanı olmayan kişiler (denetçiler, bağımsız değerlendiriciler, danışmanlar ve hizmet alınan firmaların çalışanları) internet erişimi hizmetinden faydalanabilmek için; hangi birimde çalışıyorlarsa o birimin yöneticilerinin uygun görüşüyle ve kendilerine açılacak geçici kullanıcı adlarıyla internet’e erişebileceklerdir.

**E-posta Kullanımı**

1. Tüm Ajans çalışanlarının kurumsal e-posta kullanma hakkı bulunmaktadır.
2. Kullanıcıların Ajans politikalarına uygun olarak giden ve gelen mesajları virüs korumasından geçmekte ve içerik denetimine tabi tutulmaktadır.
3. Kullanıcılar kendilerine ait kullanıcı adı ve şifre ile e-posta servislerini kullanmalıdır. Kullanıcılar başkasına ait kullanıcı adı ve şifre ile e-posta servisini kullanmamalıdır.
4. Kurumsal E-posta(cka.org.tr uzantılı) sistemi sadece iş süreçleri için kullanılırken; mesaj ile ekli dosyalarının içeriği de buna uygun olmalıdır. E-posta içeriğinin sorumluluğu kullanıcıdadır. Dolayısıyla uygun olmayan şekilde kullanımlardan (örneğin, Ajansı lekeleyen e-posta gönderimi, tacizkar kullanım, propaganda amaçlı kullanım, eğlence amaçlı kullanım vb.) kullanıcı sorumlu tutulacaktır. Uygun içerik olsa dahi iş amacı dışında kişisel iletişimde kurumsal e-posta kullanılmayacak, forumlar ve sosyal ağlara kurumsal e-posta ile üye olunmayacaktır.
5. Kullanıcı e-posta kullanırken, e-postanın içerdiği bilginin hassasiyet seviyesine uygun olarak, sadece bu bilgiye erişim yetkisi olan kişilere e-posta göndermelidir.(Örn, yürütülmekte olan bir projeyle ilgili gönderilecek mail, o projenin koordinatörüne ya da yetkili temsilcisine gönderilmelidir.)
6. Kullanıcı kendisine gelen bir e-postayı ilet (forward) seçeneğini kullanarak başka kullanıcı/kullanıcılara yönlendirmeden önce; e-posta içeriği ve eklerinin uygunluğunu kontrol etmelidir. Bu kontrol alıcının içerikteki bilgiye erişmesinin sakıncalı olduğu durumların oluşmaması için gereklidir.
7. Gizli bilgileri içeren belgeler ek bir koruma olmadan e-posta ile gönderilmemelidir.
8. E-posta kullanımında grup tanımlamaları ile birden fazla kişiye aynı anda e-posta gönderebilme imkanı bulunmaktadır. Kullanıcı; iş süreçleri için gerekli olmadığı durumlarda, kullanıcılara ve/veya bu gruplar kullanılarak grup üyelerine e-posta göndermemelidir.
9. Kullanıcılar Ajans dışından ve/veya Ajans içinden kendilerine gelen şüpheli mesajlar için “Anti-virüs Yazılımı Kullanımı ve Zararlı Kodlardan/Virüslerden Korunma” başlığında belirtilen uygulama esaslarına uygun davranmalıdır. Kullanıcılar aldıkları e-postalarda virüs olabileceği şüphesiyle hareket etmeli ve tanımadıkları kişilerden gelen mesajları, konu (subject) alanında anlamsız sözler taşıyan şüpheli mesajları, göndereni tanıyorsa da, konusu ya da metninde mantıksız bilgiler içeren e-postaları açmamalı, bir nedenle e-posta şüpheli görünüyorsa, açmadan göndereni arayarak sorulmalıdır.
10. Sürekli istenmeyen(spam) e-posta alınan adresler Bilgi İşlem Sorumlusuna bildirilerek gelen maillerin bloke edilmesi sağlanabilir.
11. Gelen mailler bilgisayarda kurulu Outlook kısmına çekilerek mail serverda alan işgal etmemelidir.

**Anti-Virüs Yazılımı Kullanımı ve Zararlı Kodlardan/ Virüslerden Korunma**

1. Güncel ve standart virüs tarama sistemi, Ajans’ın tüm bilgisayarlar ve yerel alan ağında kullanılmaktadır. Gelen ve giden e-postalar güvenlik ürünleri ile taranmaktadır.
2. Makineler üzerinde yüklü olan anti-virüs tarayıcılar sayesinde tarama işlemleri otomatik olarak yapılmaktadır.
3. Şüpheli veya yetkisiz kaynaklardan gelen dosyalar ve güvenilmeyen iletişim ağlarından gelen dosyalar, kullanılmadan önce art niyetli yazılımlara karşı kontrol edilmelidir.
4. Kullanıcılar bilgisayarlarına müdahale etmemeli, bilgisayarlarında yüklü olan anti-virüs yazılımını kapatma girişiminde bulunmamalıdır.
5. Bilgi sistemleri kullanıcıların, kesinlikle, bilgisayarın belleğine, dosya sistemine veya yazılımına zarar verecek, kendini kopyalatacak, veya başka şekilde performansını olumsuz etkileyebilecek bilgisayar kodu yazmamalı, oluşturmamalı, çalıştırmamalı, kopyalamamalı veya yaymamalıdır.
6. Bilgisayarlar USB/CD ile boot (içinde USB veya CD varken bilgisayarın açılması) edilmemelidir.
7. Alınan bütün tedbirlere rağmen bilgi sistemlerine zaman zaman virüs girmesi ve bilgi sistemlerine zarar vermesi mümkündür. Bilgisayarınıza virüs girdiyse daha az etkilenmenin de çeşitli yolları bulunmaktadır. Bu durumla karşılaşıldığında, virüs bulaştıysa sorunu kullanıcı kendisi çözmeye çalışmamalı Bilgi İşlem Sorumlusuna başvurarak teknik destek almalıdır.

Personel Adı Soyadı:

Görev Unvanı:

İmza: