BİLFEN ŞİRKETLER TOPLULUĞU

BİLGİ VE SİSTEM GÜVENLİĞİ POLİTİKALARI BİLDİRİMİ

Bilgi ve Sistem Güvenliği Politikalarında yer alan **Kurum** ifadesi *Bilfen Şirketler Topluluğunu*, **Kullanıcı** ifadesi *Bilfen Şirketler Topluluğunda görevli her kademedeki tüm personeli* içerir.

Bilgi ve Sistem Güvenliği Politikaları, Kurumdaki tüm personel ile kendilerine herhangi bir nedenle Kurum bilişim kaynaklarını kullanma yetkisi verilen **paydaş** *(kurum ile işbirliği yapan firma personeli)* ve **konuk**ların *(kurum müşteri ve/veya ziyaretçilerinin)* uyması gereken kural ve politikaları içerir.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele edilmesi Hakkında Kanun kapsamında hukuki süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla, Kurumca uygun görülen sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının iz kayıtları, ajanlı veya ajansız iz toplama yöntemleri kullanılarak toplanır ve en az 6 ay süreyle Kurumca saklanır.

Teknolojik değişikliklere ya da Kurumun genel politikasındaki ve hizmetlerindeki değişikliklere göre bu politikada gerekli düzenlemeler Bilfen Bilişim Teknolojileri Departmanınca yapılır. Tüm Kurum personeli Bilfen Bilişim Teknolojileri Departmanınca yayınlanan "Bilgi ve Sistem Güvenliği Politikaları" nı takip etmekle yükümlüdür.

Sorumluluk

Kurum personelinin, çocukların cinsel istismarına, müstehcenliğe, şiddet ve intihara yönlendirmeye, uyuşturucu ve uyarıcı madde kullanımını özendirmeye yönelik internet sitelerine girmesi, sohbet oturumları açarak kuruma ait gizli bilgileri paylaşması, oyun oynaması, devlet büyüklerine hakaret etmesi; gazete, forum ve benzeri sitelerde kurumu küçük düşürücü ve kamuoyunu yanıltmaya yönelik yorumlar yapması, özel hayatına ilişkin suç oluşturabilecek nitelikteki bilgi ve işlemleri kurum internet hattı üzerinden yapması ve sair cezai müeyyide gerektiren davranışlarından kaynaklı her türlü cezai ve hukuki sorumluluk kendisine aittir.

Genel kurallar

(1) Kullanıcı, bilgi teknolojileri kapsamındaki **bilişim kaynaklarına** *(Bilfen tarafından kurulup yönetilen her türlü bilgisayar/bilgisayar ağı ve bu ağa bağlanan elektronik cihaz ile diğer donanım, yazılım ve servislere)* zarar veremez, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunamaz, içeriğini izinsiz olarak değiştiremez.

(2) Kullanıcı, bilgi teknolojileri kapsamındaki herhangi bir kaynağı, kendisinden başka hiç kimse adına ve yararına kullanamaz veya bir başkasının kullanımına izin veremez.

(3) Kullanıcı, başka kullanıcıların bilgisayarında yer alan şifrelendirilmiş paylaşım alanlarına çeşitli yöntemleri kullanarak erişemez ve bu türlü girişimlerde bulunamaz.

(4) Kullanıcı, çalışmalarının sonlandırılması ile birlikte kendisinde bulunan bilgisayar, yazıcı, disk ve benzeri tüm donanım ve malzemeleri, tüm yazılım ürünleri ve kodları ile bilişim sistemleri kullanımına yönelik tüm şifreleri içeren Kurumun tüm bilişim varlıklarını iade eder. Kullanıcının bilgi ve bilgi işlem olanaklarına erişim hakları kaldırılır.

(5) **Yüklenici firma** (*kurumun donanım/yazılım/hizmet aldığı firma*) personeli, ancak sistem yöneticisi veya görevlendirdiği bir personel nezaretinde ve kontrolünde çalışma yapar. Nezaret eden kurum personeli yapılan çalışmaları kayıt altına alır ve herhangi bir olumsuzluk durumunda bu olumsuzluğu açıklayıcı rapor sunmak zorundadır.

(6) Gizlilik içeren bilgiler ile kişisel veriler, kanunen yetkili sayılan merciler dışında hiçbir kişi, kurum ya da kuruluş ile paylaşılmaz.

Aktif dizin hizmetleri kuralları

Aktif Dizin, internet ağındaki kaynakların bilgisini tutan ve bu bilgiyi kullanıcılara ve uygulamalara sunan ağ hizmetidir. Ağ kaynaklarına ulaşmak, bu kaynakları isimlendirmek ve güvenli bir şekilde yönetmek için gereken ortamı sağlamak amacıyla oluşturulur.

(1) Kurum bünyesinde çalışmakta olan veya işe başlayan her personel ile paydaş ve konuklar için aktif dizin kullanıcı hesabı açılır.

(2) Kullanıcı, kendisine verilen "kullanıcı adı"nı ve "şifresi"ni bir başkası ile paylaşamaz ve bir başkasına kullandıramaz. Kullanıcı, "kullanıcı hesabına" ait geçici şifresini derhal değiştirerek, “Şifre Politikası” na uygun olarak şifresini oluşturur.

(3) Kullanıcının Kurumca belirlenecek periyotlarla "kullanıcı şifresini" değiştirmesi gerekir. Kullanıcı şifresini yenilemeyen veya kullanıcı şifresini üst üste birkaç kez hatalı giren kullanıcının kullanıcı hesabı geçersiz kılınır ve iletişim ağına giriş izni otomatik olarak kaldırılır. İlgililerin başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.

(4) Her bir kullanıcı, bilgisayarda kendi "kullanıcı adı" ve "şifresi" ile oturum açarak çalışır. Çalışması biten kullanıcı, oturumu veya bilgisayarını kapatarak bilgisayara başkalarının fiziksel erişimini engeller. Bilgisayar başından kısa süreli ayrılmalarda bilgisayar oturumunu kilitler.

(5) İlgili hesabın amacı dışında kullanılması ve bu hesaptan doğabilecek zararların sorumluluğu, hesabı kullanan kullanıcıya aittir.

E-posta işlemleri kuralları

(1) Kullanıcı, e-posta adresi olarak, Kurumca kendisine tahsis edilen adresi kullanır. Bunun dışındaki e-posta servisleri kurum işlemlerinde kullanılmaz.

(2) Kullanıcı, kurum saygınlığını zedeleyecek ve/veya başkalarını taciz edecek kurum içi veya kurum dışı e-posta gönderemez. E-posta adresi internet üzerinde herhangi bir siteye kurumsal amaçlar dışında abone olmak için kullanılamaz.

(3) Kullanıcı, Kurum tarafından kendisine tahsis edilen e-posta adresini sohbet yapmak için kullanmaz.

(4) Kullanıcı, hesabını ticari ve kâr amaçlı olarak kullanamaz. Bu amaçla çok sayıda kullanıcıya toplu halde reklam, tanıtım, duyuru ve benzeri amaçlı e-posta gönderemez ve zincir e-posta, sahte e-posta ve benzeri zararlı e-postalara yanıt yazamaz.

(5) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmaz ve derhal silinir.

(6) Kullanıcı, kendisine ait e-posta adresinin şifresinin güvenliğinden ve bu e-posta adresinden gönderilen e-postalardan doğacak hukuki işlemlerden sorumludur. Şifresinin başkası tarafından tespit edildiğini fark ettiği andan itibaren derhal Bilfen Bilişim Teknolojileri Departmanıyla temasa geçip, departmanı durumdan haber etmekle yükümlüdür.

Şifre politikası

(1) Kullanıcı, kurumda kullanılan ve belirli bir şifre ile girilmesi zorunlu olan her türlü uygulama için şifre belirler.

(2) Kullanıcının şifrelerini belirlerken dikkat edeceği kurallar şunlardır:

a) Şifreler en az 6 karakter olmalıdır.

b) Şifreler küçük harf, büyük harf, rakam ve simgelerin kullanıldığı karışık yapıda olmalıdır.

c) Şifrelerin Kurumca belirlenecek sayıda hatalı girilmesi sonucu, kullanıcı hesabı Kurumun politikalarına bağlı olarak kilitlenebilir. İlgililerin başvurması halinde ilgili personelin bağlı bulunduğu birim yetkilisi ve Bilişim Teknolojileri Departmanı Yöneticisi tarafından uygun görülenlerin hesabı tekrar aktif hale getirilir.

ç) Şifreler en geç altı ayda bir değiştirilir.

d) Şifreler herhangi bir kişi ile paylaşılmaz.

Temiz masa - temiz ekran politikası

(1) Sistemlerde kullanılan şifreler, masa üstü veya ekran üstü gibi herkes tarafından görülebilecek yerlere yazılmaz.

(2) Personel, bilgisayarını belli bir süre kullanmadığı zaman otomatik olarak şifre ile oturum açmasını gerektirecek şekilde ayarlar.

(3) Kullanıcı, bağlı bulunduğu birim tarafından belirlenen gizli bilgi içeren evrakı ağ üzerinden paylaşmaz, gizli bilgi içeren atık evrakı imha eder.

(4) Personel, bilgisayarındaki, USB belleğindeki, harici diskindeki ve benzeri veri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. USB veya harici diske gizli/önemli verilerin konulması gerekiyorsa kriptolanarak/şifrelenerek saklanır.

Ağ ve internet kullanımı politikası

(1) Tüm kullanıcılar interneti bilinçli bir şekilde kullanmak, başkalarının hakkını ihlal edici ve bilişim sisteminin işleyişini engelleyici, bozucu faaliyetlerde bulunmamakla yükümlüdür.

(2) Kullanıcılar;

a) Kurum sunucuları üzerinde kendisine tahsis edilen kullanıcı adı, şifre ve IP adresi kullanılarak gerçekleştirilen her türlü etkinlikten,

b) Kendisine tahsis edilen bilgisayar üzerinde bulundurduğu belge, yazılım gibi her türlü kaynağın içeriğinden,

c) Kurum tarafından sağlanan güvenlik programlarının aktif olarak kullanılmasından ve güncellenmesinden

sorumludur.

(3) Kullanıcılar, Kurum bünyesindeki bilişim kaynaklarını, bilgisayar ağını ve interneti;

a) Kurum ağına ve haricindeki bir sisteme, ağ kaynağına veya servisine saldırı niteliğinde girişimlerde bulunmak,

b) Diğer kullanıcılara ait verileri bozmak ya da zarar vermek, gizlilik hakkını ihlal etmek,

c) Yasaklanmış her türlü materyali *(yazılı, sözlü, görüntülü, kaydedilmiş her türlü belge)* üretmek ya da dağıtmak,

ç) Gerçek dışı, sıkıntı ve rahatsızlık verici, gereksiz endişe yaratacak materyali üretmek ve dağıtmak,

d) Başka bir kullanıcının e-posta adresini, o kullanıcının izni olmadan kullanmak,

e) Yerel, ulusal, uluslararası bilgisayarları veya hizmetleri kasıtlı olarak yetkisiz kullanmak,

f) Başkalarının telif haklarını ihlal edici konumda olan yazı, makale, kitap, film, müzik eserleri gibi materyali edinmek, yayınlamak, dağıtmak,

g) Siyasi ve ideolojik propaganda yapmak

için kullanamaz.

(4) Telif hakları ve lisansları ihlal eden, Kurum ağında yoğun ağ trafiğine sebep olan, iki veya daha fazla kullanıcı arasında veri paylaşmak için kullanılan noktadan noktaya (Peer-to-peer - P2P) uygulamaları kullanılmaz. Dosya paylaşımı, anlık mesajlaşma programları ve yoğun ağ trafiğine sebep olan uygulamalar gerekli görüldüğünde Kurum tarafından filtrelenir.

(5) Bilgisayarlara tahsis edilen IP numarası ve ortam erişim kontrolü adresi (MAC adresi) ile BIOS ayarları Kurum tarafından yetkilendirilmiş kişiler dışında değiştirilemez.

(6) Kurum ağına Bilgi İşlem Departmanı Sistem Yöneticisinin bilgisi dışında herhangi bir aktif ağ cihazı eklenemez.

(7) Kullanıcılar, kişisel bilişim kaynaklarını (*şahsa ait her türlü bilgisayar/bilgisayar ağı, donanımı, yazılımı ve servisleri*) kurum ağında Bilişim Teknolojileri Departmanı Yöneticisinden izin almadan kullanamaz.

(8) Kurum içinde hizmet veren sunucu, sistem veya kullanıcı bilgisayarlarına uzaktan erişim, zorunlu hallerde Bilişim Teknolojileri Departmanı Yöneticisinin onayı/izni alınarak yapılır.

Yukarıda yazılı Bilgi ve Sistem Güvenliği Politikaları Bildirimi 15.09.2014 tarihinden itibaren geçerlidir, ilgililere tebliğ olunur.