T.C.
ÇANAKKALE VALİLİĞİ

BİLGİ İŞLEM ŞUBE MÜDÜRLÜĞÜ GÖREV, ÇALIŞMA VE BİLGİ GÜVENLİĞİ POLİTİKALARI YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

Madde 1. Bu yönergenin amacı; Çanakkale Valiliği tarafından kullanılan bilişim sistemlerinin en verimli ve uygun şekilde kullanımını sağlamak, tüm bilgisayarların, yardımcı donanımların ve diğer bilgi sistemlerinin güvenli bir şekilde çalışmasını temin etmek, ağ kaynaklarından en yüksek seviyede yararlanmak ve ağ kaynaklarının güvenliğine yönelik genel kuralları belirlemektir.

Kapsam

Madde 2. Bu yönerge, Çanakkale Valiliği bilişim sistemlerini kullanan personeller ile kendilerine herhangi bir nedenle bilişim sistemlerini kullanma yetkisi verilen misafirlerin bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği, ilke ve kurallarını kapsamaktadır.

Hukuki Dayanak

Madde 3. Bu Yönerge, 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanunun 33 üncü maddesine, 08.06.2011 tarih ve 27958 sayılı resmi gazetede yer alan Valilik ve Kaymakamlık Birimleri Teşkilat, Görev ve Çalışma Yönetmeliği'ne, 23.05.2007 tarih ve 26530 sayılı Resmi Gazetede yayınlanan 5651 sayılı kanunun 6. maddesine ve İçişleri Bakanlığı Bilgi Güvenliği Politikaları Yönergesine dayanılarak hazırlanmıştır.

Tanımlar

Madde 4. Bu yönergede geçen;

Bakanlık	: İçişleri Bakanlığı'nı
Kurum	: Çanakkale Valiliği'ni
Müdürlük	: Çanakkale Bilgi İşlem Şube Müdürlüğü'nü
Sistem ve Güvenlik Yöneticisi	: Bilgi sistemleri ve bilgi güvenliği yöneticisini,
Kullanıcı	: Bilgi sistemlerini kullanan tüm kişileri,
Domain	: Sunucuya bağlanacak bilgisayarların fiziksel bağlantı adresini,
Login	: Sisteme giriş yapma kavramını,
Sunucu	: İstemci bilgisayarlardan gelen taleplere hizmet veren ana bilgisayarı,
İstemci	: Sunucuların verdiği hizmeti alan personel bilgisayarlarını,
Etki Alanı	: Sunucu ve bu sunucuya bağlı bulunan istemcileri,
Bilişim Cihazları	: Bilgisayar (taşınabilir, masaüstü, tablet, PDA…), yazıcı, tarayıcı, fotokopi, faks, telefon, santral, vb.,
Konfigürasyon	: Bir bilgisayarı oluşturan donanımın veya programların tümünü,

İfade eder.

İKİNCİ BÖLÜM

Bilgi Güvenliği ve Bilgi Sistemlerinin Genel Kullanım Politikaları

E-Posta Politikası

Madde 5. (1) E-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiştir.

a) Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.

b) Kurum ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

c) Kullanıcı, Bakanlığın e-posta sistemini taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Müdürlüğe haber verilmelidir.

d) Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçlar ile e-posta gönderilmemelidir.

e) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Müdürlüğe haber verilmelidir.

f) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

g) Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

h) Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların yollanmasından sorumludur.

(2) E-Posta ile ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.

a) E-posta kişisel amaçlar için kullanılmamalıdır.

b) Kullanıcı, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidir. Bu yüzden parola kullanılmalı ve kullanılan parola en geç 45 günde bir değiştirilmelidir. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

c) Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Müdürlüğe haber vermelidir.

ç) Kullanıcı, kurumsal mesajlarını, kurum iş akışının aksamaması için cevaplandırmalıdır

d) Kullanıcı, kurumsal e-postalarının, kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemelidir.

e) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalıdır ve tehdit unsuru olduğu düşünülen e-postalar Müdürlüğe haber verilmelidir.

f) 6 ay süreyle kullanılmamış e-posta adresleri kullanıcıya haber vermeden sunucu güvenliği ve veri depolama alanının boşaltılması için Bakanlık tarafından kapatılabilir.

g) Kullanıcı parolaları, en az 8 karakterden oluşmalı ve parolalarının içinde; en az 1 tane harf, en az 2 tane rakam ve en az 1 tane özel karakter (@,^A,+,$,#,&,/,{,*,-,],=...) içermelidir.

h) Kullanıcı, kendilerine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren Müdürlüğe haber vermelidir.

i) Kurumla ilgili yazışmalarda resmi e-posta adresleri kullanılacak, özel e-posta adresleri (msn, gmail, yahoo vb.) zorunlu olmadıkça tercih edilmeyecektir. Özel e-posta adreslerinin kullanımından doğacak olan sıkıntılar kullanıcı sorumluluğundadır.

(3) Kurumsal e-postalar Bakanlık görevlilerince hukuksal açıdan gerekli görülen yerlerde önceden haber vermeksizin denetlenebilir.

(4) Kullanıcı, e-postalarına erişirken, POP3, SMTP, HTTP vb kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokolleri kullanmamalıdır.

(5) Bakanlık, e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.

(6) Virüs, solucan, Truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslere bulaşmış e-postalar Anti-virüs yazılımları tarafından analiz edilip, içeriği korunarak virüslerden temizlenmelidir. Ağa dâhil edilmiş bilgisayarlarda ve sunucularda ağ güvenlik yöneticileri bu yazılımdan sorumludur.

Parola Politikası

Madde 6. (1) Parola Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

a) Sistem hesaplarına ait parolalar (örnek: root, administrator, enable, vs.) en geç 6 (altı) ayda bir değiştirilmelidir.

b) Kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 45 (kırk beş) günde bir değiştirilmelidir.

c) Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.

d) Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

e) Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmeli ve eğitilmelidir.

f) Kurum çalışanı olmayan kişiler için açılan kullanıcı hesapları da kolayca kırılamayacak güçlü bir parolaya sahip olmalıdır.

g) Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

(2) Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.

a) En az 8 haneli olmalıdır.

b) İçerisinde en az 1 tane harf bulunmalıdır, (a, b, C.)

c) İçerisinde en az 2 tane rakam bulunmalıdır. (1, 2, 3...)

d) İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^A,+,$,#,&,/,{,V,],=,...)

e) Aynı karakterler peş peşe kullanılmamalıdır, (aaa, 111, XXX, ababab...)

f) Sıralı karakterler kullanılmamalıdır, (abcd, qwert, asdf,1234,zxcvb...)

g) Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)

(3) Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

a) Bütün parolalar Kuruma ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.

b) Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılmamalıdır.

c) Parola kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir.

d) Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.

(4) Uygulama Geliştirme Standartları

a) Bireylerin ve grupların kimlik doğrulaması işlemini desteklemelidir.

b) Parolalar metin olarak veya kolay anlaşılabilir formda saklanmamalıdır.

c) Parolalar, şifrelenmiş olarak saklanmalıdır.

d) En az RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

Anti-virüs Politikası

Madde 7. Anti-virüs Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurumun tüm istemcileri ve sunucuları Anti-virüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak Anti-virüs yazılımı yüklenmeyebilir.

b) İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır.

c) Sistem yöneticileri, Anti-virüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.

d) Kullanıcı hiç bir sebepten dolayı Anti-virüs yazılımını bilgisayarından kaldırmamalıdır.

e) Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartabilmelidir.

f) Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.

g) Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.

h) Optik Medya ve harici veri depolama cihazları Anti-virüs kontrolünden geçirilmelidir.

i) Kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

İnternet Erişim ve Kullanım Politikası

Madde 8. Kullanıcıların internet erişimleriyle ilgili izinler ve yasaklamalar aşağıda belirtilmiştir.

a) Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemi kullanılacaktır. İlgili Kanun, Yönetmelik ve Yönergeler gereği birim amirleri ve personelleri tarafından kullanılan bilgisayarların üzerinden genel ahlaka aykırı sitelere, sosyal paylaşım sitelerine, video paylaşım sitelerine, kumar-bahis ve online oyun sitelerine, eğlence sitelerine, dosya

indirme-yükleme sitelerine ve müzik indirme-dinleme sitelerine girilmemelidir. Bu konuda gerekli önlemler Müdürlükçe alınmalıdır.

b) Etki alanı içerisindeki istemcilerde ve ağ sisteminde P2P (limewire, kazaa, emule vb.) uygulamaları kullanmayacaktır.

c) Daire Müdürleri tarafından resmi yazı ile Müdürlüğe isimleri bildirilen personeller hariç MSN, IRC, ICQ gibi mesajlaşma yazılımlarının personel tarafından kullanılması ve bu programlar aracılığıyla dosya paylaşımı yapılması yasaklanmıştır. Ancak Bakanlığımızın uygun görmüş olduğu mesajlaşma yazılımları kullanılabilir.

d) E-İçişleri uygulaması kapsamında internet erişimlerinin hızlı olması amacıyla resmi siteler haricindeki (gov.tr, edu.tr vb..) sitelere Müdürlüğümüzce gerekli görüldüğünde kısıtlama getirilecektir.

e) İnternet ağı üzerinden canlı televizyon yayınları izlenmeyecektir. Gerekli durumlarda Birim Müdürü tarafından onaylanan kullanıcı bilgisayarlarına TV kartı kurularak televizyon yayınlarını izlemeleri sağlanacaktır.

f) İş ve işlemler haricinde internet üzerinden yüksek kapasiteli dosyalar gönderilmeyecek veya indirilmeyecektir.

g) 3. şahıslar (misafirler) kuruma ait internet erişimini sadece Müdürlüğün izni ve onayı ile kullanabilirler.

h) Ancak yetkilendirilmiş kişiler internete çıkarken, Kurumun normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla, bütün servisleri kullanma hakkına sahiptir.

Sunucu Güvenlik Politikaları

Madde 9. Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.

a) Müdürlükte bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personeller sorumludur.

b) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personeller tarafından yapılmalıdır.

c) Sunuculara ait bilgilerin yer aldığı tablo oluşturulmalıdır. Bu tabloda, sunucuların isimleri, ip adresleri ve yeri, ana görevi ve üzerinde çalışan uygulamalar, işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personel(ler)in isimleri ve telefon numaraları bilgileri yer almalı ve bu tablo bir portal üzerinde bulundurulmalıdır.

d) Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.

(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.

a) Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri Müdürlüğümüzce yapılacaktır.

b) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

c) Servislere erişimler, kaydedilerek ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.

d) Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve Anti-virüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir. Anti-virüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir

onay ve test mekanizmasından geçirilmeli, sonra uygulanmalıdır. Bu çalışmalar için yetkilendirilmiş bir personel olmalıdır.

e) Sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.

f) Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

g) Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN' larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.

h) Sunucular üzerinde lisanslı yazılımlar kurulmalıdır.

i) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

(3) Sunucu gözlemleme kuralları aşağıda belirtilmiştir.

a) Sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmamalıdır.

b) Kayıtlar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.

c) Port tarama atakları düzenli olarak yapılmalıdır.

d) Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.

e) Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.

f) Denetimler, yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.

g) Sunucuların bilgileri yetkilendirilmiş kişi tarafından tutulmalı ve güncellenmelidir.

(4) Sunucu işletim kuralları aşağıda belirtilmiştir.

a) Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulmalıdır.

b) Sunucuların yazılım ve donanım bakımları Müdürlük tarafından belirlenmiş aralıklarla, yetkilendirilmiş kişiler tarafından yapılmalıdır.

c) Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.

Ağ Yönetim Politikası

Madde 10. Ağ yönetim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Müdürlükten yazılı izin ve onay alınmadan kurum ağ sistemine hiçbir cihaz bağlanamaz, bağlaması için yetkisiz kişilerden yardım alınamaz.

b) Zararlı programcıkları kurum bünyesinde oluşturmak ve internet ortamında dağıtmak yasaktır.

c) Hiçbir kullanıcı bilgisayarlarına yüklenmiş olan Anti-virüs programlarını devre dışı bırakamaz.

d) Şüpheli kaynaklardan dosya indirilmemelidir.

e) Bilinmeyen şahıslardan gelen e-posta mesajlarının ekleri bilgisayara indirilmemelidir.

f) İnternet üzerinden kullanılan oyun, borsa, mesajlaşma gibi tüm uygulamalar yasaklanmıştır.

g) Kullanıcı şifrelerini ağ üzerinden kırmaya yönelik programlar kullanılamaz.

h) Ağ sistemi üzerinde paket yakalama, izleme, değiştirme yapılmamalıdır.

i) IP değiştirmeye, Proxy kullanmaya yönelik programların kurulması veya kullanılması yasaklanmıştır.

j) Içerik filtreleme sistemince engellenmiş, kelime bazlı engellenen resmi internet siteleri hariç, sitelere erişimin açılması için sözlü talepte bulunulamaz. Bu tür talepler Müdürlükçe ilgili Vali Yardımcısının onayı alınarak yapılabilir.

k) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılmalı ve güncellemeler uygulanmalıdır.

l) Sınırsız ağ dolaşımı engellenmelidir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmalıdır.

m) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve log kayıtları tutulmalıdır.

n) Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği Müdürlük tarafından sağlanmalıdır.

o) İnternet trafiği, İnternet Erişim ve Kullanım Politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.

p) Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanmalıdır.

q) Ağ cihazları yapılandırılması Bilgi Güvenliği Yöneticisi tarafından veya Bilgi Güvenliği Yöneticisinin denetiminde yapılmalı ve değiştirilmelidir.

r) Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

s) Erişimine izin verilen ağlar, ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmeli ve yetkisiz erişimle ilgili tedbirler alınmalıdır.

t) Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.

Uzaktan Erişim Politikası

Madde 11. Uzaktan erişim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamaktadır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.

b) Uzaktan erişim güvenliği denetlenmelidir.

c) Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

d) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

e) Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.

f) Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve Anti-virüs yazılımı güncellemeler yapılmış olmalıdır.

g) Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların bilgilerinin Müdürlüğümüze bildirilmesi gerekmekte olup bu doğrultuda yürütülen projeler üzerinden yetkiler ve hesap özellikleri güncellenecektir.

h) Müdürlük personeli ihtiyaç duyulduğu durumlarda Kaymakamlıkların sunucu ve istemcilerine uzaktan erişim ile destek verebilir.

Kablosuz İletişim Politikası

Madde 12. Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.

(1) Bütün kablosuz erişim cihazları Müdürlük tarafından onaylanmış olmalı ve Müdürlüğün belirlediği güvenlik ayarlarını kullanmalıdır.

(2) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.

a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır. IEEE 802.lx erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.

b) Erişim cihazlanndaki firmwareler düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.

c) Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

d) Varsayılan SSID isimleri kullanılmamalıdır. SSID ayan bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vb.

e) Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Kurum kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Kurum kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.

f) Erişim Cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.

g) Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından Kurumun internet bant genişliğinin tüketilmesi engellenmelidir.

h) Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.

i) Kullanıcı bilgisayarlarında kişisel antivirüs ve güvenlik duvarı yazılımları yüklü olmalıdır.

j) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

Bilişim Sistemleri Yönetim ve Genel Kullanım Politikası

Madde 13. Bilişim sistemlerine sahip olma, yönetme ve bu sistemleri genel kullanım kuralları aşağıda belirtilmiştir.

a) Güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Kurumun bünyesinde oluşturulan tüm veriler Kurumun mülkiyetindedir.

b) Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanmamalıdır. Bu konuda ilgili politikalar dikkate alınmalıdır.

c) Müdürlük, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir. Denetleme esnasında bilgisayarlar ve sistemler birim amirine veya kullanıcısına haber verilerek yerinde veya Müdürlüğe ait odalarda incelenebilir.

d) Kurum bilgisayarları etki alanına dahil edilmelidir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi olmamalıdır.

e) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.

f) Kullanıcıların tamamı kullanımlarına tahsis edilen cihazların ve sistemlerin güvenliğinden sorumludurlar.

g) Müdürlüğün bilgisi ve onayı olmadan Kurum ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.

h) Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilmemelidir.

i) Bilgisayarlara lisanssız program yüklenmemelidir.

j) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

k) Kullanıcı, herhangi bir bilginin kritik olduğunu düşünüyorsa o bilgi en az (8) karakterle şifrelenmeli ve belge üzerinde GİZLİ ibaresi bulundurulmalıdır. ÇOK GİZLİ nitelikteki e-postalar veya yazılar internet erişimi bulunan bilgisayarlarda bulundurulması halinde sorumluluk kullanıcıya aittir.

l) Güvenlik ve ağ bakımı amacıyla Sistem ve Güvenlik Yöneticileri bilişim cihazlarını, sistemlerini veya ağ trafiğini gözlemleyebilirler. Bu nedenle kullanıcı bilgisayarlarına ait yönetici (administrator) şifreleri sadece Sistem ve Güvenlik Yöneticilerinde olacaktır. Kullanıcılar tarafından yönetici şifrelerini değiştirmek için herhangi bir talepte bulunulmayacaktır.

m) Kullanıcı bilgisayarlarında resmi belgeler veya çalışmalar haricinde dosya bulundurulmamalıdır.

n) Sistem ve Güvenlik Yöneticilerinin bilgisi ve onayı olmayan hiçbir cihaz ağ sistemine alınmamalıdır.

o) Tüm kullanıcılar kendilerine tahsis edilen bilgisayarların güvenliğinden sorumludurlar. Kullanıcı hatası veya ihmali neticesinde ortaya çıkabilecek kuruma veya kişiye yönelik saldırılardan kullanıcılar sorumludurlar.

p) Birimler tarafından kullanılan bilişim sisteminin ve hizmetlerinin yönetimi, denetimi ile bakım işlemleri Müdürlük koordinasyonunda yürütülür.

q) Birimlerde ihtiyacı duyulan donanım, yazılım, teknik servis hizmetleri, temin edilmeden veya kullanılmadan önce Müdürlüğün görüşü alınmalıdır.

r) Bilişim sisteminde yer alan tüm donanım ve yazılımlar kuruma ait olup, kurum hizmetlerinde kullanılmak üzere personelin kullanımına tahsis edilmiştir.

s) Müdürlük bünyesinde bulunan sunucuların yönetiminden yetkilendirilmiş Sistem ve Güvenlik Yöneticileri sorumludur. Sunucu yönetimleri sadece bu kişiler tarafından yapılacaktır.

t) İşletim sistemi konfigürasyonları Müdürlük talimatlarına göre yapılır.

u) Ağ yapısı mühendis veya yerine görevli tarafından periyodik olarak kontrol edilir.

v) Müdürlük personellerinin, teknik hizmet sundukları için birim amirinin uygun göreceği kılık ve kıyafet ile hizmet verebileceklerdir.

w) Yetkisi ve izni olmayan personeller veri güvenliği açısından sistem odalarına girmemelidir.

x) Kurum ağına erişim isteğinde bulunan kişiler Müdürlükten izin ve onay almak, ağ sistemini kurumun belirlediği standartlar içerisinde kullanmak zorundadırlar.

y) Kurum bünyesinde bulunan veya yeni alımı yapılacak bilişim cihazlarının planlaması ile dağıtımı Müdürlük ile İdari Hizmetler Müdürlüğünce koordineli olarak yapılır.

z) Bilgi güncelleme yönetim ve denetim işlemleri Müdürlük personelince yapılır.

(2) Bilişim sistemleri genel yapılandırması ile ilgili kurallar aşağıda belirtilmiştir.

a) Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Müdürlüğe haber verilmelidir.

b) 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, vb) özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.

c) Kullanıcılar tarafından gönderilen e-postalarda gereğine göre aşağıdaki şekilde bir açıklama yer almalıdır.

"Bu e-posta iş için gönderilenler hariç sadece yukarıda isimleri belirtilen kişiler arasında özel haber/eşme amacını taşımaktadır. Size yanlışlıkla ulaşmışsa lütfen gönderen kişiyi bilgilendiriniz ve mesajı sisteminizden siliniz. Türkiye Cumhuriyeti İçişleri Bakanlığı bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmemektedir.

d) Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve mümkünse dosyalar sıkıştırılmalıdır.

(3) Bilişim sistemleri aracılığıyla yapılması yasaklanan eylemler aşağıda belirtilmiştir.

a) Herhangi bir kişinin veya kurumun telif haklarının çiğnenmesi,

b) Telif hakkına sahip olan kitap veya dokümanların izinsiz kopyalanması veya dijital ortama aktarılması,

c) Lisans gerektiren uygulamaların bilgisayarlara kurulması veya CD/DVD ortamında çoğaltılması,

d) Zararlı programların bilerek ve isteyerek kullanıcı bilgisayarına, ağ bilgisayarlarına veya sunuculara bulaştırılması,

e) Bilgisayar açılış şifrelerinin, (Sistem ve Güvenlik Yöneticileri hariç) 3. şahıslara verilmesi veya kullandırılması,

f) Kullanıcı bilgisayarlarına Müdürlüğün bilgisi veya onayı dışında donanım bağlanması veya yetkisiz kişilere bağlatılması,

g) Kurum bilgisayarlarını kullanarak yasadışı eylemlerde bulunulması,

h) Ağ güvenliğini etkileyecek veya ağ iletişimini engelleyecek faaliyetlerde bulunulması,

i) Kullanıcı bilgisayarları aracılığıyla port, şifre veya ağ taraması yapılması,

j) Yönetici şifrelerinin değiştirmeye çalışılması veya yetkisiz kişilerden bu konuda destek alınması,

k) Program veya script kullanarak kullanıcıların bilgisayar erişimlerinin engellenmeye çalışılması,

l) Bilişim sistemleri hakkında 3. şahıslara bilgiler verilmesi, yetkisiz kişilerce ağ yapısına müdahale edilmesinin sağlanması,

m) Cihazların, yazılımların veya verilerin izin alınmadan kurum dışına çıkarılması veya yerlerinin değiştirilmesi,

n) Şahsi veya kurumsal USB belleklerde kurulmadan çalışan programlar bulundurulması, bu programların kurum bilgisayarlarında çalıştırılması,

o) İnternet üzerinden lisans haklarına sahip programlar indirilmesi, indirilen programların kurum bilgisayarlarına kurulması,

p) Mobil cihazların, kişisel taşınabilir bilgisayarların kurum iletişim kaynaklarından faydalandırılmak amacıyla ağ sistemine dâhil edilmesi veya bu yönde çaba gösterilmesi,

q) Ağ sistemine 3. parti şifre kırma yazılımları yüklenmiş bilgisayarların dâhil edilmesi veya bu yönde çaba gösterilmesi,

r) Kullanıcı bilgisayarlarının resmi işlemler harici yetkisiz kişilerce kullanılması,

yasaklanmıştır.

Personel Güvenliği Politikası

Madde 14. Personel Güvenliği Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.

b) Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.

c) Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.

d) Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.

e) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.

f) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.

g) İş tanımı değişen veya Kurumdan ayrılan kullanıcıların erişim hakları kaldırılmalıdır.

h) Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

i) Kurum bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.

j) Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı", rollerin ve sorumlulukların paylaştırılması ile ilgilidir. Bu paylaşım ile kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılmalıdır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamasıdır. Sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmalıdır.

k) Çalışanlar, kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar için de bu eğitim, uyum süreci sırasında verilmelidir.

l) Çalışanların güvenlik ile ilgili aktiviteleri izlenmelidir.

m) Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

Donanım, İşletim Sistemi, Yazılım ve Teknik Destek Hizmetleri Politikası

Madde 15. Donanım, İşletim Sistemi, Yazılım ve Teknik Destek Hizmetleri politikaları ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurum ağ sisteminde yer alan tüm bilişim cihazlarına ait envanter bilgileri takip edilmekte olduğundan Müdürlüğün bilgisi dışında yetkisiz kişiler tarafından bilişim cihazlarına teknik destek verilmemeli veya bakım-onarım-değişiklik yapılmamalıdır.

b) Bilişim cihazları enerji tükettiğinden uzun süre kullanılmayacakları durumlarda kapalı tutulmaları gerekmektedir. Bilişim cihazlarının verimli kullanılması esas olduğundan mesai bitiminde kapatılmaları gerekmektedir. Açık bırakılan cihazların uğrayacağı zararlardan kullanıcılar ve birim amirleri sorumludurlar.

c) Bilgisayarlardaki ekran ve disk enerji kullanım ayarları ve yazıcılardaki enerji tasarruf ayarları ekonomik moda göre ayarlanmalı, azami elektrik tüketim tasarrufuna dikkat edilmelidir.

d) İzin verilen erişimlerin güvenlik önlemleri Sistem ve Güvenlik Yöneticileri tarafından alınacaktır.

e) Gereksiz servisler ve uygulamalar Müdürlük personeli tarafından kaldırılacaktır.

f) Güvenlik ile ilgili kayıtlar (loglar) Sistem ve Güvenlik Yöneticileri tarafından takip edilecek ve Müdürlük amiri ile birlikte değerlendirilecektir. Gerekli görülen tedbirler kullanıcılara bildirilmeksizin uygulanabilecektir.

g) Ağ sisteminin ve bağlı dış sistemlerin denetimi Sistem ve Güvenlik Yöneticisi tarafından uzaktan erişim yolu ile yapılabilecektir.

h) Kullanıcılar, kendilerine tahsis edilen bilişim cihazlarının data ve güç kablolarının hasar görmemesi için gerekli tedbirleri almak zorundadırlar.

i) Bilişim cihazlarının bağlı bulunduğu elektrik sistemine kullanımı yasak olan ısıtıcı, soba, elektrikli çaydanlık, vantilatör gibi özel kullanım amaçlı cihazlar kesinlikle bağlanamaz. Bu tür cihazların kullanımından kaynaklanacak arızalardan kullanıcılar ve birim amirleri sorumludurlar.

j) Kullanıcılar taleplerini ve sorunlarını kendi birim sorumlularına iletecek, birim sorumluları da Müdürlük amirine bildireceklerdir.

k) Bakım veya destek talepleri karşılanan kurum personeli Müdürlük personeli tarafından doldurulacak olan Bakım ve Onarım Formu' nu imzalayacaktır.

l) Kurum birimlerinde bilgisayar donanımı, yazılımı, ağ bağlantısı, internet vb. hizmetlerle ilgili yaşanan arızalara Müdürlük personeli tarafından müdahale edilebilecektir.

m) Müdürlük personeli haricinde müdahale edilen bilgisayar etki alanından çıkartılarak, söz konusu bilgisayar sistem odasına alınır ve detaylı bir incelemeden geçirilir. Tutulacak olan yetkisiz müdahale ile ilgili tutanak Müdürlük amirine teslim edilir.

n) Birimlerden format atılması sebebiyle alınan veya gönderilen bilgisayarlar içerisinde bulunan ve söz konusu bilgisayarın kullanıcısı tarafından konumları belirtilen veriler Müdürlük personeli tarafından yedeklenecektir. Kullanıcı tarafından doğru konumu belirtilmeyen ve yedeklenemeyen verilerin kaybolması durumunda sorumluluk söz konusu bilgisayarın kullanıcısına aittir.

o) Yedekleme ve geri yükleme esnasında veriler içerisinde yasaklanmış programcıklar veya zararlı yazılımlar tespit edilmesi durumunda Müdürlük personeli tarafından konuyla ilgili bir tutanak tutularak Müdürlük amirine teslim edilecektir.

p) Müdürlük personelinin kurum envanterine kayıtlı olmayan veya kurum personeline ait olan şahsi bilişim cihazlarına bakım, onarım ve teknik destek verme yükümlülüğü bulunmamaktadır.

q) Kuruma ait lisanslı yazılımların şahsi amaçlarla kullanılması kesinlikle yasaktır. Müdürlük personelinden bu yönde talepte bulunulamaz.

r) Müdürlük personeli proje geliştirme, uygulama ve network güvenlik testleri ile web güvenlik analizleri yapabilmek amacıyla kuruma ait tüm bilişim cihazlarını, ağ sistemini ve internet erişimini kısıtlama olmadan kullanabilirler ve donanım uyum araştırmalarını kendi bilgisayarları üzerinde test edebilirler.

Elektronik İmza Politikası

Madde 16. Elektronik imza ile ilgili kullanım kuralları aşağıda belirtilmiştir.

a) Kullanıcılar sahip oldukları elektronik imzanın ve pin şifresinin başkaları tarafından kullanılmasına izin verdikleri/paylaştıkları durumlarda haklarında oluşacak hukuki ve idari sonuçları kabul etmiş sayılırlar.

b) Kullanıcılar elektronik imzaları veya cihazları kaybolduğunda / çalındığında konuyu Müdürlüğe bildirmekle ve en kısa sürede yenisini temin etmekle yükümlüdürler.

c) Yeni kullanıcılar (adlarına elektronik imza gelmemiş olanlar), elektronik imzaları kaybolmuş, çalınmış veya cihazları arızalanmış olanlar hariç tüm kullanıcılar elektronik imzalarını e-içişleri sisteminde kullanmak zorundadırlar.

d) E-imza sahibi kullanıcılar kurumdan ayrılmaları halinde (emeklilik, kurum değişikliği, istifa vb.) e-imza cihazını Müdürlüğe teslim etmelidirler.

Cezai Yükümlülükler

Madde 17. Yukarıda belirtilen maddeler ile 20.02.2012 tarihli İçişleri Bakanlığı Bilgi Güvenliği Politikaları Yönergesini ihlal eden personeller hakkında adli suçlar saklı kalmak kaydı ile 657 ayılı Devlet Memurları Kanununun 125. Maddesi gereğince işlem yapılacaktır.

Yürürlük

Madde 18. Bu yönerge Çanakkale Valisinin onayladığı tarihten itibaren yürürlüğe girer.

Yürütme

Madde 19. Bu Yönerge hükümlerini Çanakkale Valisi yürütür.

OLUR

09./12/2014

Ahmet ÇINAR

Vali