

# İLETİŞİM BAŞKANLIĞI BİLGİ GÜVENLİĞİ POLİTİKALARI YÖNERGESİ

## BİRİNCİ BÖLÜM

### Amaç, Kapsam, Dayanak ve Tanımlar

#### Amaç

**MADDE 1-** (1) Bu Yönergenin amacı İletişim Başkanlığı bünyesinde bilgi ve veri güvenliği konularında gerekli önlemleri almak, politikaları, ilkeleri, usul ve esasları belirlemektir.

#### Kapsam

**MADDE 2-** (1) Bu Yönerge, Başkanlık merkez, taşra ve yurt dışı teşkilatındaki tüm personel ile kendilerine herhangi bir nedenle Başkanlık bilişim kaynaklarını kullanma yetkisi verilen diğer tüm kullanıcılar için kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

#### Hukuki dayanak

**MADDE 3-** (1) Bu Yönerge, 14 sayılı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 19 uncu maddesine dayanılarak hazırlanmıştır.

#### Tanımlar

**MADDE 4-** (1) Bu Yönerge’de geçen terimler tanımlarıyla birlikte aşağıda verilmiştir:

- Başkan: İletişim Başkanını,
- Başkanlık: İletişim Başkanlığını,
- Antivirüs: İstemcileri ve sunucuları virüs, solucan, truva atı gibi zararlı yazılımlardan koruyan yazılımı,
- BİDB: Bilgi İşlem Dairesi Başkanlığını,
- DMZ: Kurum içi ağı ile Kurum dışı ağı birbirinden ayıran yapıyı,
- Firmware: Sayısal veri işleme yeteneği bulunan donanımların kendisinden beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımı,
- Güvenli kanal: Güçlü bir şifrelemeye sahip iletişim kanalını,
- Güvenlik duvarı (Firewall): Bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemini,
- IP: İnternet Protokolü; ağdaki cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve veri alışverişinde bulunmak için kullandıkları benzersiz bir numarayı,
- IPSec (Internet Protocol Security) VPN: Genel ve özel ağlarda şifreleme ve filtreleme hizmetlerinin bir arada bulunduğu ve bilgilerin güvenliğini sağlayan iletişim kuralı ile uç kullanıcıya güvenli uzaktan erişim sağlayan protokolü,
- Kullanıcı: Başkanlık merkez, taşra ve yurt dışı teşkilatındaki tüm personel ile kendilerine herhangi bir nedenle Başkanlık bilişim kaynaklarını kullanma yetkisi verilen diğer tüm kullanıcıları,
- LDAP (Light weight Directory Access Protocol): Aktif dizin ve e-posta gibi programlardan bilgi almak için kullanılan ağ protokolünü,

- j) MAC adresi: Bir ağ cihazının tanınmasını sağlayan kendisine özel adresi,
- k) Ortak klasör (Public Folder): Başkanlık içi bilgileri toplamaya, düzenlemeye ve başka kişilerle paylaşma olanağı sağlayarak ortak ilgi alanlarında bilgi paylaşımı sağlayan yapıyı,
- l) RADIUS (Remote Authentication Dialin User Service): Sunuculara uzaktan bağlanan kullanıcılar için kullanıcı adı-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolünü,
- m) Risk: Başkanlık bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörleri,
- n) Sahte e-posta: Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanmak ve kişisel bilgilerine (tamamen yasadışı yoldan) erişilmesi için kullanılan e-postayı,
- o) SNMP: Bilgisayar ağları üzerindeki birimleri denetlemek amacıyla tasarlanmış protokolü,
- ö) Spam: Yetkisiz ve/veya istenmeyen reklam içerikli e-postayı,
- p) SSL (Secure Socket Layer): Ağ üzerinde güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolünü,
- r) Sunucu (Server): Herhangi bir ağ üzerinde bir programı veya bir bilgiyi farklı kullanıcılara, sistemlere paylaştıran ve dağıtan donanım ve yazılıma verilen genel ismi,
- s) Şifreleme: Veriyi istenmeyen kişilerin anlayamayacakları bir biçime dönüştüren özel bir algoritmayı,
- ş) Uygulama sunucusu: Herhangi bir ağ üzerinde bir programı veya yazılımı farklı kullanıcılara paylaştıran ve dağıtan bilgisayara verilen genel ismi,
- t) Uzaktan erişim: Başkanlık ağına ve bilgisayarlarına uzaktan erişim sağlama ve fiziksel olarak bağlıymış gibi ağ üzerinden veri alışverişinde bulunmayı,
- u) Veri tabanı: Birbirleriyle ilişkili bilgilerin kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde depolandığı veri topluluğunu,
- ü) VLAN (Virtual LAN): Sanal yerel ağ; birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubunu,
- v) VPN: Bir ağa güvenli bir şekilde uzaktan erişimi sağlayan teknolojiyi,
- y) Yedekleme: Verilerin/dosyaların veya veri tabanının başka bir yere kopyalanması işlemini,
- z) Yetkilendirme: Çok kullanıcıli sistemlerde sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verilmesini,
- aa) Zincir e-posta: Bir kullanıcıya gelen e-postanın art arda diğer kullanıcılara gönderilmesini,
- ifade eder.

## İKİNCİ BÖLÜM

### Bilgi Güvenliği Tanımı, Kapsam ve Hedefler

#### Bilgi güvenliği tanımı

**MADDE 5-** (1) Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve “gizlilik”, “bütünlük” ve “erişilebilirlik” olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik ögesinden herhangi biri zarar görürse güvenlik zafiyeti oluşur.

a) Gizlilik: Bilginin yetkisiz kişilerin eline geçmesini engelleme ve yetkisiz erişime karşı korunmasıdır.

b) Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.

c) Erişilebilirlik: Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

(2) Bilgi güvenliği kavramı birbiriyle bağımlı bu üç unsurun bir arada sağlanması anlamına gelir. Bu unsurlara ek olarak bilgi güvenliği açıklanabilirlik, inkâr edememe ve güvenilirlik gibi özellikleri de kapsar.

#### Bilgi güvenliğinin önemi ve kapsamı

**MADDE 6-** (1) Başkanlık yararlanıcılarının bilgi varlıklarına zamanında, eksiksiz, doğru ve kesintisiz biçimde ulaşması büyük önem taşımaktadır. Başkanlık için bilgi, değerli ve korunması gereken bir varlıktır. Bilginin gizliliği, bütünlüğü ve gerektiği zamanda hazır ve hizmette olması Başkanlığın hizmet kalitesi ve imajı ile doğrudan ilgilidir.

(2) Bilgi Güvenliği; bilgi varlıkları, uygulama yazılımları, sistem yazılımları, ağ cihazları, güvenlik cihazları, sunucular, bilgisayarlar, iletişim donanımı ve veri depolama ortamlarını içeren fiziksel varlıklar ile iklimlendirme ve kablolama gibi unsurlardan oluşan bilişim ile ilgili tüm varlıkları kapsamaktadır.

#### Bilgi güvenliğinin hedefi

**MADDE 7-** (1) Bilgi Güvenliği şartlarını yerine getirerek, çalışanların bilgi güvenliği farkındalıklarını arttırmak ve Başkanlığın temel faaliyetlerinin en az kesinti ile devam etmesini sağlamak, kurumsal riskleri en alt seviyeye indirerek Başkanlığın güvenliği ile güvenilirliğini ve imajını korumaktır.

#### Bilgi güvenliği ilkeleri

**MADDE 8-** (1) Başkanlığın bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes aşağıdaki ilkelere uymakla yükümlüdür. İlkelerin uygulama detayı bu Yönergede yer alan politikalarda belirtilmiştir.

a) Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde çalışanlar Başkanlık bilgilerinin gizliliğini korur.

b) Çok gizli, gizli, hizmete özel bilgiler gerekli güvenlik önlemi alınmadan posta, faks veya elektronik ortamda aktarılmaz. Yine bu seviyedeki bilgiler, izinsiz kişilerin eline geçme riski olduğundan, cep telefonu, sesli mesaj, telefon gibi ortamlarda kaydedilmez.

c) Çok gizli, gizli, hizmete özel güvenlik seviyesine sahip bilgi varlıklarına sahip

kişiler, bu varlığın bilmesi gerekenlerden başkasının görmemesini sağlamakla yükümlüdür.

ç) Bilgi kritiklik seviyesine göre bu Yönergede ilgili politikada belirtildiği şekilde yedeklenir.

d) Risk düzeylerine göre güvenlik önlemleri alınır.

e) Bilgi güvenliği ihlalleri personelin kendi biriminde raporlanır ve Olay Bildirim Formu ile beraber BİDB'ye bildirilir.

f) Başkanlığı ilgilendiren konularda kitap, broşür, bilgi notu, cd, slayt, taşınır bellek, haber, kupür, telefon konuşması, e-posta, mesaj vb. Başkanlık içi bilgi kaynakları yetkili amirden izin alınmadan paylaşılmaz.

g) Başkanlık bilişim kaynakları yasalara ve ilgili diğer mevzuata aykırı faaliyetler amacı ile kullanılmaz.

ğ) Tüm Başkanlık personeli kendi yükümlü oldukları iş ve işlemlerin yürütülmesinde kullandıkları bilgi sistemleri ile ilgili bilgi güvenliğinden sorumludur.

h) Her kullanıcı güvenlik tehditlerini önlemek, saptamak ve bu sorunları çözmek için işbirliği içinde ve zamanında hareket eder.

ı) Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına zarar veremez, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunamaz.

i) Personel, görevinin bitmesiyle kendisine zimmetli bilgisayar, yazıcı, disk ve benzeri tüm donanım ve malzemeleri, tüm yazılım ürünleri ve kodları ile bilişim sistemleri kullanımına yönelik tüm şifreleri içeren Başkanlığa ait tüm bilişim varlıklarını iade eder ve yetkili merci tarafından kişinin bilgi ve bilgi işlem olanaklarına erişim hakları kaldırılır.

## ÜÇÜNCÜ BÖLÜM

### Bilgi Güvenliği Politikaları

#### **Bilgi sistemleri genel kullanım politikası**

**MADDE 9-** (1) Bilgi sistemlerine sahip olma ve bu sistemleri genel kullanım kuralları aşağıda belirtilmiştir:

a) Başkanlığın güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Başkanlığın bünyesinde oluşturulan tüm veriler Başkanlık mülkiyetindedir.

b) Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanmaz. Bu konuda Başkanlığın belirlediği ilgili politikalar dikkate alınır.

c) Başkanlık, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme ve internet trafik raporlarını depolama hakkına sahiptir.

ç) Başkanlık bilgisayarları etki alanına dâhil edilir. Etki alanına bağlı olmayan Başkanlık dışı kişisel bilgisayarlarda yerel ağ kullanılmaz, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi olamaz.

d) Başkanlığa ait bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmaz ve kopyalanamaz.

e) Başkanlıkta BİDB'nin bilgisi ve onayı olmadan Başkanlık ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulamaz.

f) BİDB personeli ve ilgili teknik personel haricindeki yetkisiz kişilerce ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlara müdahale edilemez.

g) Bilgisayarlara lisanssız program yüklenemez.

ğ) Gereksizce bilişim sistemleri kaynakları paylaşımına açılmaz. Paylaşımına açılması durumunda da mutlaka güçlü bir şifre oluşturulur ve işin bitiminde de iptal edilir.

### **E-posta politikası**

**MADDE 10-** (1) Bu politika ile kullanıcıların elektronik ortamlarda haberleşirken yüksek seviyede bilgi güvenliğinin sağlanması amaçlanmaktadır. E-posta Politikası ile ilgili kurallar aşağıda belirtilmiştir. Burada yer almayan hususlarda İletişim Başkanlığı E-Posta Kullanım Politikası hükümlerine riayet edilir.

a) Başkanlığın e-posta kaynakları, Başkanlık iş ve işlemleri için kullanılır.

b) Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul eder, Başkanlık çıkarlarıyla çelişen veya normal operasyon ve iş aktivitelerini engelleyecek şekilde kullanamaz, uygunsuz içeriği saklayamaz, kötü amaçlı ve kişisel çıkarlar ve uygun olmayan içerikleri (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajlar, ticari amaçlı vb.) bağlantı olarak vermek, erişmek veya göndermek için kullanamaz.

c) Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderdiği e-postalardan doğacak idari yaptırımlardan ve hukuki işlemlerden sorumludur.

ç) Kullanıcı e-posta parolasının kırıldığını fark ettiği anda BİDB'ye haber verir.

d) Kullanıcılar, e-posta sistemini kullanmak için gerekli kimlik bilgilerini başkalarına veremez.

e) Kullanıcı, kurumsal e-postalarının, Başkanlık dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engeller.

f) Başkanlık e-posta kaynakları; reklam, aldatma, karalama vb. istenmeyen mesajlar (SPAM) göndermek için kullanılamaz. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmaz. Bu tür özelliklere sahip bir mesaj alındığında BİDB'ye bilgi verilir.

g) Kaynağı bilinmeyen oltalama (phishing), kullanıcı kodu/parolasını girilmesini isteyen, zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında açılmadan, başkalarına iletilmeden, herhangi bir işlem yapmaksızın ([some@iletisim.gov.tr](mailto:some@iletisim.gov.tr)) adresine iletilir.

ğ) Kullanıcılar, saklanması gereken e-postaları kendi bilgisayarlarında yedekler.

h) Gizli nitelikli e-posta mesajları veya mesajla birlikte gönderilmiş dosyalar sisteme kaydedilmez. Kaydedilmesi durumunda, sorumluluk kullanıcıya aittir.

ı) 6 ay süreyle kullanılmamış e-posta hesapları, kullanıcıya haber vermeden sunucu güvenliği için BİDB tarafından pasif hale getirilir.

i) Kullanıcılar, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul eder ve suç teşkil edebilecek, tehditkâr, yasadışı, hakaret, küfür veya iftira içeren, ahlaka aykırı mesajların gönderilmesinden sorumludur.

### **Parola politikası**

**MADDE 11-** (1) Parola kullanımını kullanıcı hesapları için ilk güvenlik aşamasıdır. Bu politika ile güçlü bir parola oluşturulması, oluşturulan parolanın korunması ve değiştirilme sıklığı hakkında standart oluşturulması amaçlanmaktadır. Parola Politikası ile ilgili kurallar aşağıda belirtilmiştir. Burada yer almayan hususlarda İletişim Başkanlığı Parola Yönetimi Politikası hükümlerine riayet edilir.

a) Kritik sistemlere ve ağ cihazlarına erişim için sistem yöneticileri tarafından 'Administrator' ve 'root' gibi genel sistem hesapları kullanılmaz. Bunun mümkün olmadığı durumlarda varsayılan parolalar değiştirilir.

b) Kullanıcı hesaplarına ait parolalar en geç 90 (doksan) günde bir değiştirilir. Parola yenileme işlemi esnasında son 3 parola ile aynı olmayan bir parola girilir.

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

ç) Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmez.

d) Kullanıcı, parolasını başkası ile paylaşmaz, kâğıtlara ya da elektronik ortamlara yazması durumunda güvenliğini sağlar.

e) Kullanıcı, güçlü bir parola oluşturmak için, aşağıda belirtilen maddelere uyar:

1) En az 8 haneli olmalıdır.

2) İçerisinde en az 1 tane küçük ve 1 tane büyük harf bulunmalıdır. (a, b, A, B ...)

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

4) İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !, ?, #, vb.)

5) Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, bbbb ...)

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

7) Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (aileden birisinin, arkadaşının, sahip olduğu bir hayvanın ismi, arabanın modeli, doğum tarihi, adres, telefon vb.)

f) Bütün parolalar Başkanlığa ait gizli bilgiler olarak düşünülür ve kullanıcı, parolalarını hiç kimseye paylaşmaz.

g) Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki “parola hatırlama” seçeneği kullanılmaz.

ğ) Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilir.

### **Antivirüs politikası**

**MADDE 12-** (1) Bu politika ile istemcilerin ve sunucuların virüs algılama ve engelleme standardına sahip olması için gerekliliklerin belirlenmesi amaçlanmaktadır. Antivirüs Politikası ile ilgili kurallar aşağıda belirtilmiştir:

a) Başkanlığın tüm istemcileri ve sunucuları güncel anti-virüs yazılımına sahip olmalıdır. Ancak sunucu yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak anti-virüs yazılımı yüklenmeyebilir.

b) Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasını ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasını ve uygulanmasını sağlar.

c) Kullanıcı hiçbir sebeple antivirüs yazılımını bilgisayarından kaldıramaz.

ç) Antivirüs güncellemeleri antivirüs sunucusu üzerinden yapılır. Sunucular internete sürekli bağlı olup sunucuların veri tabanları otomatik olarak güncellenir. Etki alanına bağlı

istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılır.

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

e) Bilinmeyen veya şüpheli kaynaklardan dosya indirilemez.

f) Başkanlığın ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilir.

g) Harici veri depolama cihazları her kullanımda anti-virüs kontrolünden geçirilir.

### **İnternet erişim ve kullanım politikası**

**MADDE 13-** (1) Bu politika ile internet kurallarına, etiğe ve yasalara uygun kullanımının sağlanması ve güvenli internet erişimine sahip olunması için gereken standartların belirlenmesi amaçlanmaktadır. İnternet Erişim ve Kullanım Politikası ile ilgili kurallar aşağıda belirtilmiştir:

a) Kullanıcıların internet erişimlerinde firewall, anti-virüs, URL filtreleme vs. güvenlik kriterleri uygulanır.

b) Başkanlık politikaları doğrultusunda içerik filtreleme sistemleri kullanılır. İstenilmeyen siteler (oyun, kumar, şiddet içeren vs.) yasaklanır.

c) Başkanlığın ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılır.

ç) Kullanıcılar internete BİDB tarafından sağlanan kullanıcı adı/şifre (LDAP vb.) ile erişir. Ayrıcalıklı erişim yetkileri ihtiyaç halinde gerekçelendirilerek BİDB tarafından belirli bir süre ile sınırlı olarak verilir.

d) Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmez.

e) İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmez ve indirilmez. Bu konuda gerekli önlemler alınır.

f) Uygunsuz materyal içeren yasaklı sitelere çeşitli uygulamalar kullanarak erişmek yasaktır.

g) Hizmet kalitesinin sağlanması amacıyla Başkanlık uygulamaları erişimde önceliklendirme yapılarak internet erişimi ve bant genişliğinde düzenleme yapılabilir.

ğ) Başkanlık içerisinden yapılan internet erişimlerinde 4/5/2017 tarihli ve 5651 sayılı Kanun gereği BİDB ilgili erişim bilgilerini tutmak ve devletin ilgili mercileri tarafından istenmesi durumunda bu bilgiyi sağlamakla yükümlüdür. BİDB, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgileri hukuki olarak yetkilendirilmiş kişilere verebilir.

### **Sunucu güvenlik politikaları**

**MADDE 14-** (1) Sunucularla ilgili sorumluluklar ve kurallar aşağıda belirtilmiştir:

a) Başkanlıkta bulunan sunucuların yönetiminden, BİDB'deki yetkilendirilmiş personel sorumludur.

b) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri BİDB'deki sorumlu personel tarafından yapılır.

c) Sunuculara ait bilgilerin yer aldığı tablo oluşturulur. Bu tabloda, sunucuların isimleri, IP adresleri ve yeri, ana görevi ve üzerinde çalışan uygulamalar, işletim sistemi sürümleri ve

yamaları, donanım, kurulum, yedekleme, yama yönetimi işlemlerinden sorumlu personelin isimleri ve telefon numaraları bilgileri yer alır ve bu tablo güvenli erişilebilir bir ortamda bulundurulur. Tüm bilgiler, sistem yöneticisinin belirlediği sorumlular tarafından güncel tutulur.

ç) Kullanılmayan servisler ve uygulamalar kapatılır.

d) Servislere erişimler kaydedilir ve erişim kontrol yöntemleri ile koruma sağlanır.

e) Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs vb. koruma amaçlı yazılımlar sürekli güncellenir. Antivirüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılır.

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

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

ğ) Sunucular fiziksel olarak korunmuş sistem odalarında bulunur.

h) Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, taban güçlendirmeleri yapılmış ortamlarda bulundurulur.

ı) Sistem odalarına giriş ve çıkışlar erişim kontrollü olur.

i) Sunucuların yazılım ve donanım bakımları belirli periyotlarla yapılır.

#### **Ağ cihazları güvenlik politikası**

**MADDE 15-** (1) Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir:

a) Ağ cihazlarının güncel envanter ve topoloji bilgileri tutulur, bu bilgilere erişim yetkileri olan kullanıcıların listesi oluşturulur.

b) Özel durumlar haricinde yerel kullanıcı hesapları kullanılmaz. Ağ cihazları kimlik tanımlama için (LDAP, RADIUS veya TACACS+ gibi) güvenli protokollerden birini kullanır.

c) Cihazlara erişim için güçlü bir parola kullanılır. Erişim parolaları varsayılan ayarda bırakılmaz.

ç) Yazıcı, fotokopi cihazı, faks cihazı gibi cihazların bulunduğu ağlar kritik sistemlerin bulunduğu ağlardan ayrılır.

d) Tüm ağ cihazları, BİDB’in bilgisi ve izni ile Başkanlık sistemine kurulur.

e) Yazılım ve firmware güncellemeleri önce test ortamlarında denir, daha sonra çalışma günlerinin dışında üretim ortamına taşınır.

f) Cihazlar üzerinde kullanılmayan servisler kapatılır.

g) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik kablolar) ve diğer cihazların portları etiketlenir.

#### **Ağ yönetim politikası**

**MADDE 16-** (1) Bir ağ ortamında kullanılan sistemlerin ve bu sistemler üzerinde saklanan her türlü verinin korunması ancak etkin bir ağ güvenliği denetimi ile yapılabilir. Ağ Yönetim Politikası ile ilgili kurallar aşağıda belirtilmiştir:

a) Ağ cihazları yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrılır.

b) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılır ve güncellemeler uygulanır.

- c) Ağ trafiği düzenli olarak izlenir ve ölçülür.
- ç) Sınırsız ağ dolaşımı engellenir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup ihtiyaca göre açılır.
- d) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınır ve kayıtlar tutulur.
- e) Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılır. Başkanlık kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılır ve ağlar arasında geçiş güvenlik duvarı (firewall) üzerinden sağlanır.
- f) Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Başkanlığın güvenlik politika ve standartlarıyla uyumlu olmalıdır.
- g) Ağ cihazları görevleri dışında başka bir amaç için kullanılmaz.
- ğ) Ağ cihazları yapılandırılması BİDB denetiminde yapılır ve değiştirilmez.
- h) Ağ dokümantasyonu hazırlanır ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanır.

### **Uzaktan erişim politikası**

**MADDE 17-** (1) Uzaktan Erişim Politikası ile ilgili kurallar aşağıda belirtilmiştir:

- a) İnternet üzerinden Başkanlık ağına erişen kişiler ve/veya kurumlar güvenli protokoller kullanır. Web tabanlı uygulama erişimleri sadece yetkili yöneticilere bir üst amirinin onayı ile Başkanlık tarafından verilir. Sunucu tabanlı erişimler (RDP, SSH) iş sürekliliği kapsamında ihtiyaç halinde verilir. RDP, SSH ve VPN haricinde sadece Başkanlığın belirlediği uygulama üzerinden erişim sağlanır.
- b) Uzaktan erişimler BİDB tarafından kayıt altına alınır.
- c) Başkanlık personeli bağlantı bilgilerini hiç kimse ile paylaşmaz.
- ç) Başkanlığın ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olamaz.
- d) Başkanlık personeli haricinde üçüncü şahıslara istisnai durumlar dışında uzaktan erişim izni verilmez.
- e) Başkanlık ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncel olur.
- f) Başkanlık ile ilişkisi kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri BİDB'ye bildirilir, yetkiler ve hesap özellikleri buna göre güncellenir.

### **Kablosuz iletişim politikası**

**MADDE 18-** (1) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir:

- a) Başkanlığın kablosuz bilgisayar ağına bağlanan bütün cihazların erişim bilgileri BİDB tarafından kayıt altına alınır.
- b) Bütün kablosuz erişim cihazları, BİDB tarafından belirlenen güvenlik ayarlarını kullanır.
- c) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir:
  - 1) Kablosuz cihazlar güçlü şifreleme protokolleri kullanır.
  - 2) Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Başkanlık etki alanı kullanıcı adı ve parolası bilgilerini girmeleri sağlanır ve Başkanlık kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenir.

3) Erişim cihazları üzerinden gelen kullanıcılar ağ güvenlik duvarı üzerinden ağa dâhil olur.

4) Kullanıcı bilgisayarlarında güncel anti-virüs ve işletim sistemi güvenlik duvarı yazılımlarının yüklü olması gerekir.

5) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenir.

6) Üçüncü şahısların kablosuz internet erişimleri için misafir ağ erişimi verilir.

### **Kimlik doğrulama ve yetkilendirme politikası**

**MADDE 19-** (1) Kimlik Doğrulama ve Yetkilendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir:

a) Başkanlık bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama ve sistemler üzerindeki kullanıcı yetkileri belirlenir ve denetim altında tutulur.

b) Erişim hakları tanımlanırken ihtiyacı kadar ilkesi göz önünde bulundurulur.

c) Üçüncü tarafların tüm erişimleri kayıt altına alınır. İşi biten firmaların hesapları kapatılır.

ç) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulur, tekrarlanan başarısız erişim istek ve girişimleri incelenir.

d) Kullanıcı hareketlerini doğru bir şekilde kayıt altına almak için her kullanıcıya kendisine ait bir kullanıcı hesabı açılır.

e) Son kullanıcıların yetkileri, içinde buldukları grup politikasına göre belirlenir.

### **Veri tabanı güvenlik politikası**

**MADDE 20-** (1) Veri tabanı sistemleri için güvenlik kuralları aşağıda belirtilmiştir:

a) Veri tabanı sistemleri envanteri dokümante edilir ve bu envanterden sorumlu personel tanımlanır.

b) Veri tabanı işletim kuralları belirlenir ve dokümante edilir.

c) Veri tabanı sistem kayıtları tutulur ve BİDB tarafından izlenir.

ç) Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilir.

d) Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılır ve uygun yedekleme politikaları oluşturulur, yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli olarak alınması kontrol altında tutulur.

e) Yedekleme planları dokümante edilir.

f) Manyetik kartuş, DVD veya disk ortamlarında tutulan log kayıtları en az 2 (iki) yıl süre ile güvenli ortamlarda saklanır.

g) Veri tabanı erişim politikaları “Kimlik Doğrulama ve Yetkilendirme” politikaları çerçevesinde oluşturulur.

ğ) Hatadan arındırma, bilgileri yedekten dönme kuralları oluşturulur ve dokümante edilir.

h) Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulur.

ı) Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilir.

i) Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulur ve sonrasında ilgili uygulama kontrolleri gerçekleştirilir.

j) İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenir.

k) Veri tabanı sunucusu sadece ssh, rdp, ssl ve veri tabanının orijinal yönetim yazılımına açık olmalıdır; bunun dışında ftp, telnet vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır. Ancak ftp, telnet vb. açık metin şifreli bağlantılar veri tabanı sunucudan dışarıya yapılabilir.

l) Uygulama sunucularından veri tabanına rlogin vb. şekilde erişilemez.

m) Arayüzden gelen kullanıcılar bir tabloda saklanır, bu tablodaki kullanıcı adı ve şifreleri şifrelenir.

n) Veri tabanına bağlanacak kişilerin kendi adlarına kullanıcı adı verilir ve yetkilendirme yapılır.

o) Bütün kullanıcıların yaptıkları işlemler kaydedilir.

ö) Veri tabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenir.

p) Veri tabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilir. Veri tabanı sunucularına ancak yetkili kullanıcılar erişir.

r) Veri tabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapamaz. İstekler arayüzden sağlanır. Veri tabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

### **Yazılım geliştirme politikası**

**MADDE 21-** (1) Yazılım Geliştirme Politikası ile ilgili kurallar aşağıda belirtilmiştir:

a) Başkanlık içinde geliştirilmiş/geliştirilecek yazılımlar ve seçilen paket yazılımlar ihtiyaçları karşılamalıdır.

b) Yazılım geliştirmede, analiz, tasarım, geliştirme, test ve bakım safhalarını içeren sağlıklı bir metodoloji kullanılır.

c) İhtiyaçlar, uygun bir şekilde tanımlanır.

ç) Başkanlıkta kişisel olarak geliştirilmiş yazılımların kullanılması engellenir.

d) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilir ve onaylanır.

e) Yazılımların uygulama ortamına aktarılma kararı BİDB tarafından verilir.

f) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulur.

g) Yazılımlar sınıflandırılır ve envanterleri çıkarılarak muhafaza edilir.

ğ) Yazılım konfigürasyon yönetimi yapılır, yazılım ile ilgili tüm dosyalar sunucularda saklanır, hassas bilgi olarak nitelendirilir, erişim yetkileri ve erişimleri kayıt altına alınır.

h) Parametrelerin manipüle edilmesinin önlenmesi için http post kullanılır.

ı) Güvenli ve performanslı yazılım geliştirme standartları ve isimlendirme standartlarına uyulur ve yazılım modüler yapıda geliştirilir. Bu standartlara göre kod gözden geçirme yapılarak geliştirilen kodlar uygulamaya alınır.

i) Test aşamasında modül, fonksiyon, entegrasyon ve yetkisiz erişimi engellemek için erişim testleri yapılır.

### **Değişim yönetimi politikası**

**MADDE 22-** (1) Değişim Yönetim Politikası ile ilgili kurallar aşağıda belirtilmiştir:

- a) Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri yazılı hale getirilir.
- b) Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilir.
- c) İş kritik bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek sistem ve uygulamalar BİDB tarafından belirlenir ve yazılı hale getirilir.
- ç) Yapılacak değişiklikler öncelikle mümkünse bir test ortamında denir.
- d) Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulur ve güncel tutulur.
- e) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanır.
- f) Sistemlerde oluşacak problemlere yönelik bakım, onarım, yama, güncelleme ve değişiklikler ile ilgili çalışmalardan önce varlık sahibine ve proje paydaşlarına bilgi verilir. Sonrasında ilgili uygulama kontrolleri gerçekleştirilir.

### **Bilgi sistemleri yedekleme politikası**

**MADDE 23-** (1) Bilgi Sistemleri Yedekleme Politikası ile ilgili kurallar aşağıda belirtilmiştir:

- a) Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgileri ve kurumsal veriler düzenli olarak yedeklenir.
- b) Veri yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri döneceği kritiklik derecesine göre belirlenir ve yazılı hale getirilir.
- c) Yedek medyaları mümkün olduğunca verilerin olduğu fiziksel ortamlardan farklı yerlerde veya binalarda güvenli bir şekilde saklanır.
- ç) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanır.
- d) Son kullanıcılar kendi bilgisayarlarındaki verilerin yedeklenmesinden kendileri sorumludur.

### **Bakım politikası**

**MADDE 24-** (1) Bakım Politikası ile ilgili kurallar aşağıda belirtilmiştir:

- a) Başkanlık sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınır. Bunun için gerekli bütçe ayrılır.
- b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanır.
- c) Firma teknik destek elemanlarının bakım yaparken bu Yönergeye uygun davranmaları sağlanır ve kontrol edilir.
- ç) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak “Değişim Yönetimi Politikası” ve ilişkili standartlar uygulanır.
- d) Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenir.
- e) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda, bu Yönerge uyarınca hareket edilir. Güvenlik açıkları Başkanlık Siber Olaylara Müdahale Ekibine ([some@iletisim.gov.tr](mailto:some@iletisim.gov.tr) adresine) bildirilir.

f) Başkanlık içinde firmalar tarafından bakımı ve onarımı yapılan sistemlerde, bakım işlemi yetkili bir çalışanın gözetiminde yapılır ve sistemden bilgi alınmasına engel olunur.

g) Depolama ortamının (örn. sabit disk) bakım, onarım gibi amaçlarla Başkanlık dışına çıkarıldığı durumlar kayıt altına alınır ve firma yetkilisi tarafından imzalanır. Gerekli durumlarda firma ile gizlilik sözleşmesi imzalanır.

### **Son kullanıcı güvenliği politikası**

**MADDE 25-** (1) Son Kullanıcı Güvenliği Politikası ile ilgili genel kurallar aşağıda belirtilmiştir:

a) Başkanlık intranet uygulamalarını kullanan kullanıcılar, sistemlere etki alanları dâhilinde kendilerine verilmiş kullanıcı adı ve şifreleri ile bağlanır.

b) Her bir son kullanıcının yalnızca bir adet kullanıcı hesabı olur.

c) Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşır ve internete çıkabilir.

ç) Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı 5651 sayılı Kanun'a uygun olarak kayıt altına alınır.

d) Güvenlik zafiyetlerine karşı, son kullanıcılar kendi hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi kendilerine ait bilgilerin gizliliğini korur ve başkaları ile paylaşmaz.

e) Son kullanıcılar bilgisayarlarındaki ve sorumlusu oldukları cihazlardaki verilerden kendileri sorumludur.

f) Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka bilgisayar ekranlarını kilitler.

g) Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde harici veri depolama cihazları (e-imza ve kart okuyucusu, bellek ve/veya harici hard disk gibi taşınabilir medya araçları) bırakmaz.

ğ) Son kullanıcılar, mesai bitiminde bilgisayarlarını ve çevre donanımlarını (yazıcı, monitör, hoparlör...) kapatır.

h) Başkanlık, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulayabilir.

ı) Başkanlık, son kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişiklikleri merkezi grup politikalarıyla engelleyebilir.

i) Temiz masa, temiz ekran ilkesi benimsenir ve hayata geçirilir.

j) Kullanıcılar, Başkanlık mevcut envanteri haricindeki donanımları Başkanlık bilgisayarlarında kullanmamaya özen gösterir.

k) Bilinmeyen veya şüpheli kaynaklardan dosya indirilmez.

l) Dosya paylaşım alanı ihtiyacı olması durumunda sadece Başkanlığın dosya sunucusu üzerinden yetkilendirilmiş personele erişim izni verilir. Bunun dışında paylaşım yapılmaz.

### **Fiziksel güvenlik politikası**

**MADDE 26-** (1) Fiziksel Güvenlik Politikası ile ilgili kurallar aşağıda belirtilmiştir:

- a) Başkanlık binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilir.
- b) Kurumsal bilgi varlıklarının dağılımı ve bulundurulmuş bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanır ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilir.
- c) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilir.
- ç) Kritik bilgilerin bulunduğu alanlara girişler kontrolü akıllı kartlar veya biyometrik sistemler ile yapılır ve izlenir.
- d) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanır.
- e) Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanır.
- f) Kritik sistemler özel sistem odalarında tutulur.
- g) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine, yangın ve benzeri felaketselere karşı korunur ve iklimlendirilmesi sağlanır.
- ğ) Fotokopi, yazıcı vs. tür cihazlar çalışma olmadığında kullanıma kapatılır, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınır.
- h) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilir.
- ı) Hassas bilgilerin bulunduğu alanlar (kimlik doğrulama kartı ve PIN koruması gibi yöntemlerle) yetkisiz erişime kapatılır.
- i) Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınır ve uygulanır.
- j) Yedeklenmiş materyal ve yedek sistemler sistem odasından yeterince uzak bir yerde konuşlandırılır.
- k) Fiziksel ortamların taşınmasında; paketleme, içeriğin fiziksel hasarlardan yeterince korunmasını sağlayacak şekilde yapılır.
- l) Acil durumlar için her zaman alternatif yol ve iletişim kanalları mevcut olmalıdır.

### **Kriz / acil durum politikası**

**MADDE 27-** (1) Bu politika Başkanlık personelinin, bilgi güvenliği ve iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dâhilinde gerekli müdahaleleri yapabilmelerine yönelik standartları belirlemektedir. Acil Durum Politikası ile ilgili kurallar aşağıda belirtilmiştir:

- a) BİDB personeli arasından acil durum sorumluları ve bunların yetki ve yükümlülükleri belirlenir.
- b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınır. Problem durumlarında sistem, kesintisiz veya makul kesinti süresi içerisinde felaket kurtarma veri merkezi veya aynı veri merkezi üzerinden çalıştırılır.
- c) Bilişim sistemlerinin kesintisiz çalışmasının sağlanması için sistemler tasarlanırken minimum sürede iş kaybı hedeflenir.
- ç) Acil durumlarda Başkanlık içi işbirliği gereksinimleri tanımlanır.

- d) Acil durumlarda sistem kayıtları incelenmek üzere saklanır.
- e) Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulur.
- f) Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilir.
- g) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulur ve bu bildirim süreçleri öncesinde tanımlanır.
- ğ) Acil durumlarda bilgi güvenliği yöneticisine erişilir, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilir ve zarar tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülür.
- h) Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilir.

## **DÖRDÜNCÜ BÖLÜM**

### **Çeşitli Hükümler**

#### **Yürürlük**

**MADDE 28-** (1) Bu Yönerge onayı tarihinde yürürlüğe girer.

#### **Yürütme**

**MADDE 29-** (1) Bu Yönerge hükümlerini İletişim Başkanı yürütür.