T.C.
MALTEPE ÜNİVERSİTESİ
BİLGİ İŞLEM ve SİSTEM GÜVENLİĞİ YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

Madde 1- Bu Yönergenin amacı Maltepe Üniversitesi internet ve bilgisayar ağı ile bütünleşen bilişim kaynaklarının kullanımına yönelik uyulacak kural, yetki ve sorumluluklara ilişkin usul ve esasları belirtmektir.

Kapsam

Madde 2- Bu Yönerge, Üniversite bünyesindeki akademik, idari ve teknik birimlerde çalışan tüm personel ve öğrencilerle kendilerine herhangi bir nedenle bilişim kaynaklarını kullanma yetkileri verilen paydaş ve konukların, Üniversiteye ait tüm birimlerde kullandıkları her türlü bilişim ve iletişim araçlarıyla gerçekleştirdikleri faaliyetleri kapsar.

T.C. Maltepe Üniversitesi internet erişiminde Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) "ULAKNET KULLANIM POLİTİKASI"na ve "ISO27001 Bilgi Güvenliği Yönetim Sistemi"ne tabi olduğundan, kullanıcılar Üniversitenin bilgisayar ve iletişim kaynaklarını kullanmakla aşağıda belirtilen esasları kabul etmiş sayılırlar.

Dayanak

Madde 3- Yönerge, dayanağını; 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5237 sayılı Türk Ceza Kanununun İkinci Kısım (Kişilere Karşı Suçlar), Dokuzuncu Bölüm, Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar (m.132, 133, 135, 136, 137, 138, 139, 140) Üçüncü Kısım (Topluma Karşı Suçlar), Onuncu Bölümünde (Bilişim Alanında Suçlar) 243, 244, 245, 246 maddeleri, 5070 sayılı "Elektronik İmza Kanunu" ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile 2547 sayılı Kanunun 12. maddesinden alır.

TANIMLAR

Madde 4- Bu Yönergede geçen:

a) **BİDB**: Bilgi İşlem Daire Başkanlığını,

b) **Bilişim destek hizmeti**: Üniversitenin bilişim kaynaklarının kurulumu, geliştirilmesi, kullanıma sunumu, bakımı, onarımı ve diğer teknik desteklerle Rektörlükçe belirlenen yetki ve sorumluluk düzeylerinde Bilgi İşlem Dairesi Başkanlığı ve bilişim kaynaklarını kullanıma sunan birimlerce yerine getirilen hizmetleri,

c) **EBYS:** Üniversitenin Elektronik Belge Yönetim Sistemini,

ç) **Genel Sekreterlik:** Maltepe Üniversitesi Genel Sekreterliğini,

d) **Erişim:** Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,

e) **ISO27001 Bilgi Güvenliği Yönetim Sistemi:** Bilgi güvenliğini kurmak, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasını,

f) **Konuk:** Üniversitede bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemleri üzerinde hiçbir şekilde yetkilendirilmemiş olan kişilerle görev yeri dışında çalışan kullanıcıları,

g) **Kullanıcı**: Maltepe Üniversitesi Bilişim kaynaklarını eğitim-öğretim, araştırma, yönetim ve hizmet faaliyetleri çerçevesinde kullanan Üniversitenin idari yapısı içinde yer alan birimlerde akademik ve idari görevlerde bulunan kadrolu, sözleşmeli ve geçici personelle Üniversitenin toplam olarak dört düzeydeki öğrencileriyle bilişim kaynaklarını kullanma yetkisi verilen tüm paydaşları,

ğ) **Kullanıcı hesabı**: Üniversite sunucularındaki bilişim kaynaklarını kullanmak üzere kendilerine tahsis edilen "kullanıcı adı/şifre" ikilisini,

h) **Kullanıma sunan birimler**: Bilişim kaynaklarını kullanıma sunan akademik birimlerle (Enstitü, Fakülteler, Yüksekokullar, Meslek Yüksekokulu, Konservatuvar, Uygulama ve Araştırma Merkezleri, UNESCO Kürsüleri, Bilimsel Koordinatörlükler,), uygulama alanlarını (laboratuvarlar, kütüphane, hastane) ve idari birimleri (Genel Sekreterlik, Yazı İşleri Müdürlüğü, Daire Başkanlıkları, Müdürlükler, Sürdürülebilirlik Ofisi, Bilim İletişimi Ofisi, İdari Koordinatörlükler),

ı) **Maltepe Akademik Ağı**: Marmara Eğitim Köyü Yerleşkesiyle diğer yerleşkelerdeki bilgisayar ağını,

i) **MÜBİS**: Maltepe Üniversitesi Bilgi Sistemi Mülkiyet hakları Üniversiteye ait olan, Üniversite tarafından lisanslanan ya da Üniversitenin kullanım hakkına sahip olduğu her türlü bilgisayar/bilgisayar ağı, bilgisayar donanımı, bilgisayar yazılımı ve hizmetlerin tümünü,

j) **Paydaş:** Ortak çalışma yapılan kurum ve kuruluşları,

k) **Rektörlük**: Maltepe Üniversitesi Rektörlüğünü,

l) **Sunucu**: Program veya bir bilgiyi farklı kullanıcılara/sistemlere paylaştıran/dağıtan donanım ve yazılımı,

m) **Üniversite**: Maltepe Üniversitesini,

n) **Yapı İşleri ve Teknik İşler Daire Başkanlığı**: Maltepe Üniversitesi Yapı İşleri ve Teknik İşler Daire Başkanlığını,

o)**Yüklenici firma:** Üniversitenin ihale yoluyla ürün, hizmet satın aldığı ya da çeşitli işbirliği anlaşmaları yoluyla destek aldığı kuruluşları, firmaları,

ö) **Yüklenici firma personeli:** Yüklenici firmada çalışan kişi ya da kişileri,

İfade eder.

İKİNCİ BÖLÜM
Sorumluluk ve Genel Kurallar

Sorumluluk

Madde 5- (1) 5651 sayılı Kanunla (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) ve ISO: 27001 Bilgi Güvenliği Yönetim Sistemiyle bağlantılı olarak, sistemin güvenli bir şekilde işletilmesi amacıyla, BİDB uygun görülen sistemleri, uygulamaları, kullanıcı işlemlerine ilişkin bilgi sistem ağındaki veri akışının iz kayıtlarını, ajanlı veya ajansız iz toplama yöntemlerini kullanarak toplar ve ilgili kanun ve yönetmeliklerde belirtilen süre boyunca Üniversitede ve ilgili yerlerde saklar. Bu nedenle kullanıcı, kendisine ait kişisel verilerin gizli kalması ve korunması kuralına dayalı olarak, Maltepe Akademik Ağı üzerinden gelen ve giden tüm trafik bilgilerinin önceden kullanıcıya haber verilmeksizin Üniversitece kayıt altına alınacağını ve denetlenebileceğini, bu bilgilerin istatistik, raporlama ve inceleme amaçlı olarak kullanabileceğini kabul eder.

(2) Üniversite personelinin ve öğrencilerinin, çocukların cinsel istismarına, müstehcenliğe, şiddet ve intihara yönlendirmeye, uyuşturucu ve uyarıcı madde kullanımını özendirmeye yönelik internet sitelerine girmesi, sohbet oturumları açarak Üniversiteye ait gizli bilgileri paylaşması, oyun oynaması, devlet yetkililerine hakaret etmesi; sosyal medya, gazete, forum ve benzeri sitelerde Üniversiteyi küçük düşürücü ve kamuoyunu yanıltmaya yönelik yorumlar yapması, özel hayatına ilişkin suç oluşturabilecek nitelikteki bilgi ve işlemleri Üniversite internet hattı üzerinden yapmasıyla ilgili cezai ve hukuki sorumluluğu kendisine aittir. Üniversite yukarıda belirtilen davranışları tespit etmeye ve önlemeye yönelik erişim politikalarını belirler ve uygular.

(3) Bu Yönerge kapsamında bilgi ve sistem güvenliğinin planlı, sorunsuz, güvenli ve disiplin içinde gerçekleştirilmesinden Üniversite bilişim sistemlerinden yararlanan tüm Üniversite personeli birinci derecede görevli ve sorumludur. Bu Yönerge kapsamında olup teknolojik değişikliklere ya da Üniversitenin genel politikasındaki ve hizmetlerindeki değişikliklere göre bu politikada gerekli düzenlemeler Üniversite Senatosunca yapılır ve genel ağ sayfasında "Bilgi Güvenliği Politikası" adı altında yayımlanır. Tüm Üniversite personeli yayımlanan "Bilgi Güvenliği Politikası"nı takip etmekle ve bu metinde yer alan hususlara uymakla yükümlüdür.

(4) Üniversite yasal hükümler çerçevesinde bilişim kaynaklarını ve bunlarla gerçekleştirilen faaliyetleri izleme, kaydetme ve dönemsel olarak inceleme ve denetleme hakkını saklı tutar.

(5) Üniversitenin bilişim kaynaklarında meydana gelen arızaların giderilmesi BİDB sorumluluğundadır. Yetkisiz bir müdahale söz konusu olduğunda, teknik destek verilmez ve ortaya çıkabilecek arızalar, maddi hasarlar ya da Üniversitenin ağ güvenliğinin ihlaline yol açan uygulamalardan ilgili personel sorumlu tutulur.

(6) Üniversitenin demirbaşına kayıtlı olmayan, personelin şahsi bilgisayarlarına arıza, bakım ve teknik destek hizmeti kesinlikle verilmez.

(7) Veritabanı yöneticileri MÜBİS ve diğer bilişim modüllerinde yapılan tüm sorguları kayıt altına alır ve gerekli durumlarda, sorgulamanın sebebini kullanıcıya yazılı veya sözlü olarak sorar. Kullanıcı hesabında anormal sorgu durumlarının tespit edilmesinde hesap sahibine haber verilmeye gerek duyulmadan hesabı dondurularak gerekli inceleme ve soruşturma işleminin Rektörlük veya Genel Sekreterlikçe başlatılması sağlanır.

(8) Kullanıcı herhangi bir nedenle diğer kullanıcılara ve/veya öğrencilere ait kişisel bilgileri (ad soyad, TCKN, fotoğraf, okuduğu okul, adres, telefon numarası, e-posta adresi vb.) diğer kamu kurumlarıyla ve 3. şahıslarla paylaşamaz. Gerekli görüldüğü zaman bu bilgilerin paylaşımı için Üniversiteden talepte bulunulur. Üniversite uygun gördüğü durumlarda bilgileri yasal sınırlar içerisinde ilgili kişi, kamu kurum ve kuruluşlarıyla paylaşır.

(9) Kullanıcı Üniversitenin hassas bilgilerinin ortaya çıkmasına, akademik ve idari birimlerinin ulaşılamaz hale gelmesine neden olabilecek tüm eylemlerden kaçınır.

(10) Kullanıcı, kullanımına tahsis edilen bilişim kaynaklarının güvenliğine yönelik önlemleri alır.

(11) Üniversite ağı ve bu ağı kullanan her kullanıcı ve cihazla ilgili her türlü erişim, güvenlik ve yönetim politikaları BİDB tarafından belirlenir ve uygulanır. Bu ağ üzerindeki trafik, 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) çerçevesinde gelen ve giden yönünde kaydedilerek incelenebilir ve raporlanabilir.

(12) Üniversite, gerekli durumlarda BİDB'in belirlediği erişim politikası düzenlemelerini uygular.

Genel Kurallar

Madde 6- (1) Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına (bilgisayar, ağ sistemi, sunucu sistemi, bilgi sistemleri, yazıcı, kamera, projeksiyon vb.) 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, Üniversiteyle olan bağı sona erdiğinde, kendisinde bulunan bilgisayar, yazıcı, disk vb. tüm donanım ve malzemeleri, tüm yazılım ürünleri ve kodlarıyla birlikte bilişim sistemleri kullanımına yönelik tüm şifreleri ve tüm bilişim varlıklarını Üniversiteye iade eder. Kullanıcının Üniversiteyle olan ilişkisi sona erdiği andan itibaren tüm erişim hakları kaldırılır.

(5) Yüklenici firma personeli Üniversitede BİDB başkanının gözetimi ve denetimi altında çalışır. İşbu personelce yapılacak çalışmaları gözetim altına alacak ve denetleyecek olan Üniversite personeli, en az yüklenici firma personeli kadar konusunda uzman olanlar arasından seçilir ve sistem yöneticisinin onayıyla, bu yetkilendirme kayıt altına alınır. Bu kurallara uyulmadığında doğacak sorunlardan ve/veya maruz kalınacak zararlardan Üniversite kadar ilgili yüklenici firma da sorumludur. Çalışmaları gözetim altında tutan Üniversite personeli tüm işlemleri kayıt altına alır ve herhangi bir olumsuzluk durumunda bu olumsuzluğu açıklayıcı bir raporu BİDB'e sunar.

(6) Bilgi güvenliğini etkileyen arızalar mümkün olan en kısa sürede BİDB tarafından uygun yönetim kanalları kullanılarak Genel Sekreterliğe rapor edilir.

(7) Gizlilik içeren bilgilerle kişisel veriler, e-devlet kapsamında protokol yapılarak bilgi paylaşımı yapılan veya yasal olarak yetkili sayılan merciler dışında hiçbir kişi, kurum ya da kuruluşla paylaşılmaz.

Madde 7- Bilişim kaynakları Türkiye Cumhuriyeti yasalarına, Üniversitenin yönetmelik ve yönergelerine aykırı faaliyetlerde kullanılamaz.

Madde 8- Ulusal Akademik Ağ ve Bilgi Merkezinin (ULAKBİM) ağ yönetim birimi olan Ulusal Akademik Ağ (ULAKNET) tarafından yürürlüğe konulan "Kabul Edilebilir Kullanım Politikası Sözleşmesi "ne aykırı iş ve işlemler yapılamaz.

Madde 9- Bilişim kaynaklarının herhangi bir amaçla kullanım yetkisi Rektörlüğe aittir.

Madde 10- Bilişim kaynaklarının kullanımında güvenliği bozan durumlara ve girişimlere ilişkin bilgilerin tutulması ve kullanıcı kimlik belirlemeleri için Rektörlük ve Genel Sekreterlikçe gerekli düzenlemeler yapılır.

Madde 11- Bilişim kaynaklarının kullanıma sunulması ve kullanımı, bu kaynakların kullanım amaçları çerçevesinde yapılır; kullanım amaçları tüm kullanıcılara açık bir biçimde bildirilir, kaynakların kullanım yeri ve konumu bu kaynakları kullanıma sunan birimlerin yöneticilerinden yetki ve onay alınmadan değiştirilemez.

Madde 12- Bilişim kaynakları, genel ahlak kurallarına, kişilerin ve kurumların fikri mülkiyet haklarına, veri güvenliğiyle ilgili mevzuata ve kişisel bilgilerin korunmasına aykırı olarak kullanılamaz. Ayrıca, başkalarının verilerini tahrip etmek, izinsiz erişim sağlamak, iftira atmak, karalama yapmak, Üniversitenin ve Üniversitedeki kişilerin çalışmalarını engellemek veya bozmak, istenmeyen ileti (SPAM) göndermek gibi faaliyetlerde bulunmak yasaktır. Bu tür materyallerin üretilmesi, dağıtılması veya barındırılması kesinlikle yasaklanmıştır.

ÜÇÜNCÜ BÖLÜM
Bilgi ve Sistem Güvenliği Kuralları ve Politikaları

Aktif Dizin Hizmetleri Kuralları

Madde 13- (1) Üniversitede çalışmakta olan veya işe başlayan her personelle paydaş ve konuk için aktif dizin kullanıcı hesabı açılır. Geçici süreliğine görevlendirilen paydaş ve konukların kullanımı için bağlı oldukları birimde görev yapan yetkili personel adına profili ve şifresi farklı ek kullanıcı hesapları açılır. Geçici görevli personel bu hesaptan sorumludur. Geçici görevli personelin görevlendirme süresinin sonunda ilgili hesabın şifresi değiştirilir ve bir sonraki kullanıma kadar edilgin olarak bekletilir.

(2) Kullanıcı, kendisine verilen "kullanıcı adı"nı ve "şifresi"ni bir başkasıyla paylaşmaz ve bir başkasına kullandırmaz. Kullanıcının, "kullanıcı hesabı"na ait geçici şifresini derhal değiştirerek, bu **Yönergenin 15'inci** maddesinde yer alan şifre politikasına uygun olarak şifresini oluşturur.

(3) Kullanıcının, BİDB tarafından belirlenecek periyodlarla "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. Yeniden başvurulması halinde ilgili hizmet, Genel Sekreterlik veya BİDB'in uygun görmesi durumunda tekrar ilgili kullanıcıya tahsis edilir.

(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, hesabın kullanıcısına aittir.

(6) Üniversitedeki her bir son kullanıcı ve bilgisayar Maltepe.local aktif dizin etki alanı üyesi olmalıdır. Etki alanında olmayan kullanıcı veya bilgisayarın internet erişimleri engellenir.

e-Posta İşlemleri Kuralları

Madde 14- (1) Kullanıcı, tüm resmî yazışmalarında e-posta adresi olarak, Üniversitece kendisine tahsis edilen e-posta adresini kullanır. Bunun dışındaki e-posta servislerini resmî işlerde kullanamaz.

(2) Kullanıcı, Üniversitenin saygınlığını zedeleyecek ve/veya başkalarını taciz edecek Üniversite içi veya Üniversite dışı e-posta gönderemez. e-Posta adresi internet üzerinde herhangi bir siteye Üniversitenin amaçları dışında abone olmak için kullanılamaz.

(3) Üniversite kendisine veya çalıştığı birime tahsis edilen e-posta adresini, sohbet (chat) yapmak için kullanamaz.

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

(5) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

(6) Kullanıcı, kendisine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludur. Şifresinin başkası tarafından tespit edildiğini fark eden anında, şifresini değiştirip BİDB ile temasa geçip durumu haber vermekle yükümlüdür.

(7) Güvenlik ve performans açısından e-posta eklentilerinin toplam boyutu hiç bir durumda BİDB'in belirlediği boyut değerinden fazla olamaz.

(8) e-Posta hesapları için öngörülen kotadan dolayı bir problem yaşanmaması için e-posta hesabının denetimi kullanıcıya aittir.

(9) BİDB sistem ve kullanıcı güvenliğini sağlamak amacıyla gelen giden e-postalar için politika belirleyebilir ve uygulayabilir.

(10) BİDB kişisel verilerin korunması ve gizli kalması koşuluyla gelen giden e-postalara ait istatistiksel bilgileri inceleyebilir.

(11) Gerekli görülmesi halinde BİDB kullanılan e-posta sistemleri üzerinde her türlü değişikliği yapma hakkına/yetkisine sahiptir.

(12) Üniversite personeli olma niteliğini kaybedenlerin (emeklilik, istifa, kurum değişikliği, vefat, işten çıkarılma vb.) isimleri ilgili birim tarafından BİDB'e bildirilir. BİDB belirlediği süre sonunda bu e-posta hesaplarını kapatır.

(13) Usulsüz kullanıldığı tespit edilen veya istenmeyen iletiler (SPAM), virüs yayarak sistem ve kullanıcıların güvenliğini tehdit eden e-posta hesapları devre dışı bırakılır. Kullanan hakkında gerekli yasal işlem başlatılır.

(14) Üniversitedeki akademik ve idari birimlerin talebiyle oluşturulan e-posta gruplarının üyelerinin güncel olmasından ilgili birim sorumludur. Birimin kapanması, isminin değişmesi, faaliyetin bitmesi vb. nedenlerle işlevini kaybeden e-posta grubunun kapatılması veya grup üyelerinde ekleme, çıkarma yapılması talepleri Rektörlükçe BİDB'e bildirilir.

Şifre Politikası

Madde 15- (1) Kullanıcı, Üniversitede 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 10 (on) karakter olmalıdır.

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

c) Şifrelerin üst üste hatalı girilmesi sonucunda, kullanıcı hesabı BİDB'in politikalarına bağlı olarak kilitlenebilir. İlgililerin başvurması halinde ilgili hizmet bir üst yetkilinin uygun görmesi durumunda tekrar verilir.

ç) Şifreler en geç altı ayda bir değiştirilir.

d) "Yönetici/Admin" kullanıcı şifreleri sadece sistem yöneticilerinde olur, kesinlikle son kullanıcılarla ve yüklenici firmalarla çalışıldığı zaman firma personeliyle paylaşılmaz.

e) Şifreler herhangi bir üçüncü kişiyle paylaşılamaz.

Temiz Masa - Temiz Ekran Politikası

Madde 16- (1) Sistemlerde kullanılan şifreler, masaüstü veya ekran üstü gibi herkes tarafından görülebilecek yerlere yazılamaz.

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

(3) Kullanıcı, gizli bilgi içeren evrakı ağ üzerinden paylaşmaz, gizli bilgi içeren atık evrakı imha eder.

(4) USB bellek (taşınabilir harici bellek), harici disk vb. hafıza ünitelerinin kullanım şartlarını BİDB belirler. BİDB gerekli gördüğü durumlarda ilgili ünitelerin kullanımının durdurulması, sınırlandırılması veya şifrelenmesi (kriptolanması) gibi uygulamaları yürürlüğe koyar.

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

Ağ ve İnternet Kullanımı

Madde 17- (1) Tüm kullanıcılar interneti bilinçli bir şekilde kullanmak, başkalarının hakkını ihlal edici ve bilişim sisteminin işleyişini engelleyici, bozucu faaliyetlerde bulunmamakla yükümlüdür.

(2) Kullanıcı;
a) Üniversitenin sunucuları üzerinde kendisine tahsis edilen kullanıcı adı, şifre ve IP adresi vb. kullanılarak gerçekleştirilen her türlü etkinlikten,

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

c) Bilişim sisteminin kullanımı hakkında yetkili makamlar tarafından talep edilen bilgilerin doğru ve eksiksiz verilmesinden,

ç) BİDB tarafından sağlanan güvenlik programlarının etkin olarak kullanılmasından ve güncellenmesinden,

d) Bilişim sisteminin kullanım kurallarına, kanun ve yönetmeliklerle Üniversitenin tabi olduğu mevzuata uygun olarak kullanımından sorumludur.

(3) Kullanıcı, Üniversitedeki tüm bilişim kaynaklarını;

a) Üniversite ağına ve Üniversite dışındaki bir sisteme, ağ kaynağına veya servisine saldırı niteliğinde girişimlerde bulunamaz.

b) Diğer kullanıcılara ait verileri bozamaz ya da zarar veremez, gizlilik hakkını ihlal edemez.

c) Yasaklanmış herhangi bir materyali üretemez ya da dağıtamaz.

ç) Gerçek dışı, sıkıntı ve rahatsızlık verici, gereksiz endişe yaratacak materyali üretemez ve dağıtamaz.

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

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

f) Başkalarının telif haklarını ihlal edici konumda olan yazı, makale, kitap, film, müzik eserleri vb. gibi materyali edemez, yayımlayamaz, dağıtamaz.

(4) Telif hakları ve lisansları ihlal eden, zararlı yazılım bulunduran, bilişim ağında yoğun ağ trafiğine sebep olan iki veya daha fazla kullanıcı arasında veri paylaşmak için uçtan uca uygulamalar kullanılamaz. Dosya paylaşımı, anlık mesajlaşma programları ve Üniversitenin altyapısında soruna yol açacak şekilde yoğun ağ trafiğine neden olan uygulamalarla güvenlik

tehdidi oluşturan reklam, içerik, site, kullanıcı, yazılım, uygulama, erişim sağlayan cihazların tamamı gerekli görüldüğünde BİDB tarafından filtrelenir veya erişime kapatılır.

(5) Zararlı veya güvenlik tehdidi oluşturan yazılım, uygulama, eklenti vb. içerik barındıran bilgisayarlar yeniden kurulum yapılmadan Üniversitenin ağına dahil edilemez.

(6) Bilgisayarlara tahsis edilen IP numarası ve ortam erişim kontrolü adresi (MAC adresi) ile BIOS (Temel Giriş-Çıkış Sistemi) ayarları BİDB tarafından yetkilendirilmiş kişiler dışında değiştirilemez.

(7) Üniversite ağına sistem yöneticisinin bilgisi dışında herhangi bir etkin ağ cihazı eklenemez.

(8) Kullanıcılar, kişisel bilişim kaynaklarını Üniversite ağında sistem yöneticisinden izin almadan kullanamaz.

(9) Üniversite içinde hizmet veren sunucu, sistem veya kullanıcı bilgisayarlarına uzaktan erişim, zorunlu hallerde BİDB onayı/izni alınarak yapılır.

(10) BİDB gerekli gördüğü durumlarda Üniversite içi hassas düzeydeki hizmetlere öncelik sağlamak üzere akademik ağın bant genişliğini yeniden düzenleyebilir.

(11) Akademik ağda kategorisi olmayan IP adresi, içerik veya sitelere erişim izni verilmez. Erişim talepleri Destek Modülü (destek.maltepe.edu.tr) ve EBYS üzerinden yapılır.

(12) Kullanıcı, kendi kullanıcı hesaplarıyla internet üzerinden gerçekleştirdiği tüm işlemlerden sorumludur. Kimlik bilgilerini uygun bir şekilde saklar ve başkalarıyla paylaşamaz.

(13) Üniversitenin ağ güvenliği açısından tehlike yaratabilecek nitelikte zararlı olduğu tespit edilen internet adreslerine erişim tüm kullanıcılar için engellenir. Kullanıcı bu tür engellemelerin kaldırılması konusunda BİDB'e herhangi bir talepte bulunamaz.

(14) Üniversitenin ağı üzerindeki bilgisayarlara erişim hakkı, yetkisi olmayan kişilere verilemez.

(15) Yetkilendirilmiş kişiler ve kuruluşlar dışında, ağ kaynağına veya servisine zarar verebilecek DDOS (Servis Dışı Bırakma) saldırısı, port/ağ taraması, paket dinleme, ağ izleme, IP değiştirme gibi kasıtlı veya kasıtsız girişimlerde bulunamaz.

(16) Üniversitenin bilişim kaynakları ağ ve internet kaynaklarının Üniversite dışından kullanılmasına neden olabilecek ya da Üniversite dışındaki kişi ya da bilgisayarların kendilerini Üniversite içerisindeymiş gibi tanıtmalarını sağlayacak (DHCP, DNS, Proxy, IP Sharer, NAT vb.) şekilde kullanılamaz.

(17) BİDB, Üniversitenin internet ağında erişime açılacak ve kapanacak portları belirleme ve düzenleme yetkisine sahiptir. Uzaktan erişim (rdp, ssh, telnet vb.), dosya-yazıcı paylaşımı gibi portlara ve uygulamalara erişim izni verilemez.

(18) Üniversitenin ağı üzerindeki bilgisayarlarda güvenlik politikalarının BİDB'in belirlediği antivirüs yazılımına tabi olması zorunludur.

(19) Üniversitenin bilişim kaynaklarında ve genel ağında zararlı yazılım tespit edilen, saldırmaya yönelik teşebbüste bulunan ve kullanılan güvenlik sistemlerini aşmaya, atlatmaya yönelik her türlü tünel, proxy, vpn vb. program kullanan kullanıcı veya kurumların, internet ve intranet erişimleri kesilir. İlgili durum ortadan kalkınca erişim tekrar sağlanır. Erişim politikalarını ve sistemlerini aşmaya veya bilişim sistemlerine saldırmaya yönelik girişimde bulunan kullanıcı veya kurum hakkında yasal işlem başlatılır. Ayrıca Üniversitenin bilişim sistemlerine yönelik dışarıdan VPN, proxy, tünel vb. bağlantılarla erişim sağlanması (kullanıcının kendi ip adresi yerine sahte ip adresleri üzerinden erişmesi), saldırı girişiminde bulunulması durumunda ilgili erişimler engellenir. Erişim kesintileriyle ilgili süreçleri BİDB belirler ve yönetir.

(20) BİDB onayı olmadan hiçbir yazılım satın alınamaz. Satın alınması düşünülen yazılım ve programlar için BİDB'den uygun görüş alınır.

(21) BİDB kullanıcıları sistem güvenliği ve politikaları hakkında düzenli olarak bilgilendirir ve tam bir süreklilik içinde farkındalık eğitimleri düzenler.

Sistem Odası Güvenliği

Madde 18- (1) Üniversitenin sistem odalarının nerede yer alacağı ve hangi koşulları taşıması gerektiği ilgili mevzuat uyarınca Rektörlükçe belirlenir.

(2) Sistem odasında gürültü ve titreşime karşı yalıtım önlemi sağlanır. Bakım, denetim ve acil durum çizelgeleri görünür bir panoda yer alır. Sistem odasının periyodik olarak denetimleri BİDB tarafından sağlanır ve ilgili çizelgelere işlenir.

(3) Sistem odasında kesintisiz güç kaynağı ile soğutma sistemleri kesintisiz olarak çalışır. Sistem odasında meydana gelen arıza vb. durumlarda BİDB'e bilgi verilerek en kısa sürede arızanın giderilmesi sağlanır.

(4) Sistem odalarına ilişkin iş ve işlemler BİDB ile Yapı İşleri ve Teknik İşler Daire Başkanlığının eşgüdümü çerçevesinde tasarlanır, planlanır, uygulanır, gerekli tüm önlemler birlikte alınır.

Hassas Verilerin Yedeklenmesi

Madde 19- (1) BİDB, BİDB'in kullanıcılara tahsis ettiği bilgisayarların belleğinde yer alan ve Üniversiteyle ilgili tüm iş ve işleyişleri içeren kayıtlar da dahil olmak üzere, Üniversitenin iş ve işleyişinde kullanılan bilgi sistemlerini, kullanıcı hesaplarını, web sayfalarını ve Üniversitenin belleğini oluşturan her türlü veriyi yedekler.

(2) Yedekleme sistem odasında en az iki farklı depolama alanında yapılır. BİDB yedeklenecek her türlü bilgiyi Üniversitede belirlenen yedek sistem odasındaki depolama alanına ve ayrıca Üniversitenin işleyişinde hassas öneme sahip sunucuları da bulut sistemine yedek olarak yerleştirir.

İnternet Sitesi Barındırma Hizmeti Politikası

Madde 20- (1) Üniversitenin sorumluluğunda yürütülen projelere ait internet sitelerini barındırma hizmeti Üniversite sunucuları üzerinden yapılır.

(2) İletişim için Üniversite tüzel kişiliğine ait e-posta adresi kullanılır.

(3) Üniversite onayı olmadan alan adı alınamaz. Üniversiteye ait olmayan sunucularda web hizmeti yayını yapılamaz, dosya ve veritabanı depolanamaz. Alan adı alınması gereken durumlarda Rektörlükten onay alınır ve onayın ardından http://maltepe.edu.tr/websitesi adresine web sitesi olarak kaydedilir.

(4) Üniversitenin internet sitelerinin hazırlanmasında, güncellenmesinde ve yönetilmesinde dikkat edilecek hususlar şunlardır:

a) BİDB'in belirlediği internet sitesi standartları dikkate alınır.

b) Her türlü içerikten Üniversitenin ilgili akademik ve/veya idari yöneticileri sorumludur.

c) Uygulamalara yetkisiz kişilerin erişimini engelleyen önlemler alınır.

ç) Alınan web hizmetine ait şifreler BİDB ve görevli personelin sorumluluğundadır.

d) Hassas içerikler Üniversitenin BİDB çatısı altında görevlendirdiği yetkili ya da yetkililerce güvenli bir ortamda yedeklenir.

e) Herhangi bir saldırı halinde site üzerinde bir işlem yapılmadan BİDB'e haber verilir.

f) Tahsis edilen web alanında virüs, truva atı vb. zararlı içerik veya bağlantı, oyun, yetkisiz erişime sebep olabilecek uygulamalar bulundurulmaz.

g) Yayımlanacak her türlü içerik telif hakları, fikrî haklar, şeref ve haysiyetin korunması ve gizlilikle ilgili mevzuat hükümlerine dayanmalıdır.

ğ) Yayımlanacak hiçbir içerik BİDB'in herhangi bir politikasını, kuralını ya da düzenlemesini ihlal edemez.

h) Web barındırma alanı, internet sitesi yayıncılığı dışında dosya depolama ya da arşiv alanı olarak kullanılamaz.

Nitelikli Elektronik Sertifika (e-İmza) Kullanımı

Madde 21- (1) Üniversite içi ve dışı resmî yazışmalar EBYS üzerinden güvenli elektronik imza yetkisiyle yapılır.

(2) Güvenli elektronik imza sayısal imzadır ve elle atılan imza ile aynı hukukî sonucu doğurur ve aynı ispat gücüne sahiptir.

(3) Kullanıcılar elektronik imzalarını ve şifrelerini hiç kimseyle paylaşamaz.

(4) e-İmza veya şifrenin başkasının eline geçmesi sonucunda meydana gelecek her türlü durumda, kusurun derecesine göre yasal sorumluluk e-imza sahibine aittir.

(5) e-İmzanın çalınması, kaybedilmesi durumunda sorumluluk kullanıcıya aittir ve EBYS üzerinden tekrar talep edilerek yenilenmesi zorunludur.

6) Kullanıcı sertifika sağlayıcılarından gelen e-imza güncellemelerinin tarihlerini takip eder ve güncellemeleri zamanında, e-İmzasını kullanarak yapar. Aksi takdirde ortaya çıkabilecek her türlü maddi ve hukuki sonuçtan sertifika sahibi sorumludur.

(7) Kullanıcı, EBYS'ye tanımlı kişilerin bilgi değişikliklerini EBYS'den sorumlu ilgili birime iletmekle hükümlüdür.

DÖRDÜNCÜ BÖLÜM
Uygulama ve Yaptırımlar

Yaptırım ve Uygulama

Madde 22- (1) Bilişim kaynaklarının Yönergeye aykırı olarak kullanılmasının tespiti durumunda gerçekleştirilen eylemin niteliğine, kaynaklara veya kişilere, kurumlara verilen zararın boyutuna ve tekrarına göre, İş Kanunu, 2547 sayılı Yükseköğretim Kanunu ve diğer ilgili mevzuat hükümleri uyarınca gerekli cezai işlemler Rektörlükçe uygulanır.

BEŞİNCİ BÖLÜM
Çeşitli Hükümler

Hüküm Bulunmayan Hususlar

Madde 23- Bu Yönergede hüküm bulunmayan hususlarda ilgili diğer mevzuat hükümlerine göre işlem yapılır.

Yürürlük

Madde 24- İşbu Yönerge Maltepe Üniversitesi Senatosunca kabul edildiği tarihden sonra yürürlüğe girer. (Kabul tarihi:10.07.2025)

Yürütme

Madde 25- Bu yönergenin hükümlerini T.C. Maltepe Üniversitesi Rektörü yürütür.

Yönergenin Kabul Edildiği SENATO	
Tarih	**Toplantı Sayısı/Karar Sayısı**
10.07.2025	10/09