



BİLGİ İŞLEM DAİRE BAŞKANLIĞI
İNTERNET VE YEREL AĞ SERVİSLERİ
KULLANIM YÖNERGESİ

Doküman No	YÖ-058
İlk Yayın Tarihi	20.04.2017
Revizyon Tarihi	06.06.2018
Revizyon No	01
Sayfa	1 / 7

Amaç

Madde 1 – (1) Bu Yönergenin amacı; Kırşehir Ahi Evran Üniversitesi bilgisayar ağı ve internet altyapısı ile bunlarla bütünleşen bilişim kaynaklarının kullanımına ilişkin ilkeleri belirlemektir.

Kapsam

Madde 2 – (1) Bu Yönerge, internet kullanıcılarının Kırşehir Ahi Evran Üniversitesi Bilgi İşlem Daire Başkanlığı aracılığıyla internet erişimine ve yerel ağ kullanımına ilişkin biçim ve koşullar ile Bilgi İşlem Daire Başkanlığından alınacak bilişim hizmetlerini kapsar.

Dayanak

Madde 3 – (1) Bu Yönerge, 2547 sayılı Kanununun 12 inci maddesinin 1. Fıkrasının (h) bendine dayanarak hazırlanmıştır.

Tanımlar

Madde 4 – (1) Bu Yönergede geçen;

- a) Kırşehir Ahi Evran Üniversitesi Bilişim Cihazı: Mülkiyeti veya kullanım hakkı Kırşehir Ahi Evran Üniversitesine ait olan, Kırşehir Ahi Evran Üniversitesince satın alınan veya lisanslanan bilgisayar ağı, internet altyapısı, bilgisayar sistemi, donanımı, yazılımı ve hizmetlerinin tümünü,
- b) Kırşehir Ahi Evran Üniversitesi Bilişim Kaynaklarını Kullanıma Sunan Birimler: Kırşehir Ahi Evran Üniversitesi Bilişim Kaynaklarını kullanıma sunan akademik birimler (fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, araştırma ve uygulama merkezleri, hastaneler), idari birimler (daire başkanlıkları, müdürlükler) ve spor-kültür-sosyal etkinliklerin yürütüldüğü birimleri,
- c) Başkanlık: Bilgi İşlem Daire Başkanlığını,
- d) Bilgisayar Ağı: Bilgisayarlar arasında veri/bilgi aktarımı ve etkileşimini sağlayan, geniş ve dar alanlar bütünlüğünde fiziki ağ yapısı ile bunu destekleyen ve kullanımını gerçekleştirmeye yarayan tüm donanım ve yazılımların oluşturduğu sistemi,
- e) Bilişim Destek Hizmetleri: Kırşehir Ahi Evran Üniversitesi Bilişim Kaynaklarının kurulumu, kullanıma sunumu, bakımı, onarımı ve diğer teknik destekler ile ilgili Rektörlükçe belirlenen yetki ve sorumluluk düzeylerinde Başkanlık ve Bilişim Kaynaklarını Kullanıma Sunan Birimlerce yerine getirilen hizmetlerini,
- f) İnternet Altyapısı: Ulusal ve uluslararası bilgisayar ağı üzerinde tüm kullanıcı uçlarının adres yapılarını ve veri/bilgi iletişimi kurallarını içeren belirli protokoller ile etkileşimi ve iletişimini sağlayan bir sistemi,
- g) KamuSM: Kamu Sertifikasyon Merkezini,
- h) Rektörlük: Kırşehir Ahi Evran Üniversitesi Rektörlüğünü, ifade eder.

Genel Hükümler

Madde 5- (1) Başkanlık, Kırşehir Ahi Evran Üniversitesi tüzel kişiliğini korumak ve sistemin güvenliğini sağlamak amacıyla, kanunlar ve bu Yönerge hükümleri çerçevesinde kendisine bağlı tüm bilişim cihazlarını gerek gördüğü anda her türlü hizmeti denetleyebilir ve kısıtlayıcı önlemler alabilir.



BİLGİ İŞLEM DAİRE BAŞKANLIĞI
İNTERNET VE YEREL AĞ SERVİSLERİ
KULLANIM YÖNERGESİ

Doküman No	YÖ-058
İlk Yayın Tarihi	20.04.2017
Revizyon Tarihi	06.06.2018
Revizyon No	01
Sayfa	2 / 7

- (2) Başkanlık, kullanıcıların internet ortamındaki bazı zararlı sitelere erişimini engelleyebilir, denetleyebilir ve içerik yönünden bazı dosya tiplerinin ve programların (görüntü dosyaları, ses dosyaları, kazaa, e-donkey vb. programlar) kullanılmasına engel olabilir.
- (3) Sistem ve ağ güvenliğini tehdit edecek unsurların önlenmesi amacıyla, sadece Başkanlığımızda bulunan sunuculara (WWW sunucusu, FTP sunucusu, İleti (Posta) sunucusu vb.) yerleşke dışından erişim hakkı verilmiştir.
- (4) Kullanıcılar yerleşke ağı içerisindeki bilgisayarlarında, posta ve bulut hesaplarında hukuki açıdan suç oluşturacak belgeler, kamu kurum veya kuruluşları ile gerçek/tüzel kişiler hakkında karalama belgeleri, iftira mahiyetinde olan, gerçek dışı, sıkıntı ve rahatsızlık verici her türlü doküman ve belgeyi barındıramazlar.
- (5) Kullanıcılar başka bir sistemin e-posta sunucusunu veya başka bir kullanıcının e-posta hesabını, kişinin izni olmadan ileti gönderme amacıyla kullanamazlar. Kasıtlı olarak yetkisiz kullanım, başkalarının verilerini tahrip etme, kişisel bilgilere zarar verme, başkalarına ait çalışmalarını bozmaya ve tahrip etmeye yönelik çalışmalar yapma gibi etkinliklerde bulunamazlar, ticari reklamlar ve haber duyuruları gibi istenmeyen iletiler gönderemezler.
- (6) Kullanıcıların e-posta hesaplarında ve bilgisayarlarında yer alan belgelerin ve her türlü bilginin yayın haklarından doğabilecek hukuki sorumluluklar tümüyle kullanıcıya aittir.
- (7) Kullanıcılar, yerleşke ağı içerisinde belirlenen ağ merkezlerinin dışındaki uçlara, Başkanlığın bilgisi dışında Switch (Anahtar), Access Point, Yönlendirici (Router) ve benzeri cihazlar takıp uç çoklama işlemi yapamazlar.
- (8) Kullanıcılar, birimleri içerisindeki ağ merkezinde ya da kendilerine ait olan uç arkasında IP çoğaltma işlemi yaparak, birçok bilgisayarı tek bir bilgisayar üzerinden internete çıkaramaz ve bilgisayarlarına Başkanlığın belirlediği IP grupları dışında IP numarası atayamazlar.
- (9) Kullanıcı, Başkanlıkça verilen hizmetlerden yararlanmaya başladığı andan itibaren bu belgede yer alan maddelere uyacağını kabul eder ve yükümlülüğünü üstlenir. Aksi yönde bir tutum belirlendiğinde yerel ağ, e-posta ve diğer kullanım haklarının sona erdirileceğinin ya da belirli bir süre durdurulacağını bilincindedir. Belirtilen kurallara uyulmadığında tüm hukuki ve yönetsel (idari) işlemlerden kullanıcılar kendileri sorumlu olurlar.
- (10) Kullanıcılar kullanmakta oldukları şifreleri gerçek ve tüzel kişilerle paylaşamazlar, masa üstü, ekran üstü vb. herkes tarafından görülebilecek yerlere yazamazlar.
- (11) Kullanıcılar, kendilerine tahsis edilen bilgisayarları belirli bir süre kullanmadığı zaman otomatik olarak şifre ile oturum açmasını gerektirecek şekilde ayarlamalıdır.
- (12) Kullanıcılar, kendilerine iletilen gizli bilgi mahiyetindeki bilgileri ifşa edemezler, üçüncü şahıslarla paylaşamazlar.
- (13) Kullanıcılar, USB veya harici diskte gizli/önemli verileri bulundurmaları gerekiyorsa ilgili dokümanların güvenliğini almakla sorumludurlar.
- (14) Kullanıcılar, bilişim sistemlerinin kullanımında, kanun ve yönetmelikler ile üniversitemiz tarafından çıkarılan yönergelerle uygun davranmakla sorumludur.
- (15) Başkanlık bu yönergenin dışında sistem güvenliğini sağlamak amacıyla, karşılaşılabilecek her türlü probleme karşı tedbir almaya yetkilidir.
- (16) Birimlerin; ortak kullanım alanında bulunan bilişim cihazları (bilgisayar, yazıcı, projeksiyon vb.) ilgili birimin sorumluluğu ve yetkisindedir.



BİLGİ İŞLEM DAİRE BAŞKANLIĞI
İNTERNET VE YEREL AĞ SERVİSLERİ
KULLANIM YÖNERGESİ

Doküman No	YÖ-058
İlk Yayın Tarihi	20.04.2017
Revizyon Tarihi	06.06.2018
Revizyon No	01
Sayfa	3 / 7

E-Posta İşlemleri Kullanım Politikası

Madde 6- (1) Kullanıcı E-Posta adresi olarak, Başkanlıkça kendisine tahsis edilen adresi kullanır. Bunun dışındaki E-Posta servisleri resmi işlemlerde kullanılamaz.

- (2) E-posta adresi internet üzerinden herhangi bir siteye kurumsal ve akademik amaçlar dışında abone olmak için kullanılamaz.
- (3) Başkanlık tarafından verilen e-posta servisinde ekler filtreden geçirilmekte, spam (istenmeyen ileti) ve virüs gönderen bilgisayarların IP adresleri bloklanmakta ve “.pif, .scr, .vbs” uzantılı e-posta ekleri otomatik olarak engellenmektedir. Başkanlık gerekli gördüğü hallerde bu dosya uzantılarını değiştirebilir veya yeni dosya uzantısı ekleyebilir.
- (4) Herhangi bir nedenden dolayı Kırşehir Ahi Evran Üniversitesinden ayrılan kullanıcıların e-posta adresleri ayrıldıkları tarih itibarı ile altı (6) ay içerisinde otomatik olarak silinecektir. Bu süre içerisinde ayrılan personelin tedbir almaması durumunda sorumluluk tümüyle ayrılan personele aittir.
- (5) Kaynağı bilinmeyen e-posta ekinde gelen her türlü çalıştırılabilir dosyalar (.bat, .com, .exe, .msi, vb. uzantılı) alındığında kesinlikle açılmamalı, hemen silinmeli, yanıt verilmemeli ve kesinlikle başkalarına iletilmemelidir. Ayrıca şüpheli e-postalarda yer alan linkler tıklanmamalıdır.
- (6) Çok sayıda kişiye toplu olarak gönderilen iletilerin, alıcıların birbirlerinin adreslerinin görülmemesini gerektiren durumlarda Gizli (BCC (Blind Carbon Copy)) ile gönderilmelidir.
- (7) Elektronik posta iletilerine kredi kartı numarası, herhangi bir şifre gibi özel bilgiler yazılmamalıdır.

IP Sanal Santral Kullanım Politikası

Madde 7- (1) IP telefon talepleri, ilgili birim amirinin onayına istinaden Başkanlığımıza yapılmaktadır.

- (2) Telefon tanımlamalarının yapılması, görüşmelere açılması, telefon cihazlarının kurulumlarının yapılması, telefon iletişimde devamlılığın sağlanması, telefon rehberi hazırlama ve güncelleme vb. her türlü teknik işlemler Başkanlığımız tarafından yapılır.
- (3) Üniversite içi görüşmelere açık bir telefonun, resmi görüşmelerde kullanılmak üzere Şehir içi, GSM-Şehirlerarası görüşmelere açılması talebi “Başbakanlığın 2007/3 sayılı Tasarruf Tedbirleri” gereğince birim amirinin teklifiyle alınan Rektörlük Oluru ile gerçekleştirilir.
- (4) Başkanlık tarafından kullanıcılara tahsis edilen telefonlar sadece resmi görüşmeler için kullanılacak, özel görüşmelerde kesinlikle kullanılmayacaktır.

Güvenlik Duvarı ve İçerik Filtreleme Kullanım Politikası

Madde 8- (1) Kurum bünyesinde kullanılmakta olan bilişim cihazları, bilgisayar ağı erişim ve içerik denetimi yapan bir güvenlik duvarı (firewall) üzerinden internete çıkmaktadır.

- (2) Ağ güvenlik duvarı (firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşılabileceği sorunları önlemek üzere tasarlanan bir cihazdır.
- (3) Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlamaktadır.
 - a) İçerik filtreleme sistemleri kullanılarak, istenilmeyen sitelere (şiddet içeren, kumar, pornografik vb.) erişim yasaklanmaktadır.
 - b) Saldırı tespit ve önleme sistemleri kullanılmaktadır.



BİLGİ İŞLEM DAİRE BAŞKANLIĞI
İNTERNET VE YEREL AĞ SERVİSLERİ
KULLANIM YÖNERGESİ

Doküman No	YÖ-058
İlk Yayın Tarihi	20.04.2017
Revizyon Tarihi	06.06.2018
Revizyon No	01
Sayfa	4 / 7

Güvenlik Kamera Sistemleri Kullanım Politikası

Madde 9 - (1) Üniversite güvenliğine katkı sağlanması, kampüs içerisinde oluşabilecek olumsuzluklara karşı hızlı ve etkin tedbirlerin geliştirilmesi, gerçekleşen olayların çözümüne yönelik geriye dönük kayıtların incelenmesi ve hukuki delillerin temin edilmesi, öğrencilerin toplantı ve gösteri yürüyüşlerinde, yasadışı olayları önlenmesi ve toplulukların provokasyona yönlendirilmelerine engel olunması, Üniversitemizde güvenlik hizmetlerinin sunumunda bilgi ve iletişim teknolojilerinden yararlanmak suretiyle güvenlik hizmetlerinde en ileri düzeyde yararlanılması, suç işlenmesinin önlenmesi, işlenmiş suçların takibi ile sanıkların en kısa sürede yakalanmasına katkı sağlanması amacıyla güvenlik sistemi kurulmuştur.

- (2) Üniversite binalarındaki ofis ortamları, sosyal tesisler içindeki çalışma odaları ile binaların içindeki veya dışındaki lavabo ve tuvaletler özel alanlardır. Bu alanlarda hiçbir şekilde kamera sistemi tesis edilemez, izlenemez veya görüntü kaydı yapılamaz.
- (3) İç ve dış mekânlarda bulunan kameralar görüş alanlarını 7 gün 24 saat kesintisiz kayıt yapabilmektedir. Ancak, kameraların metraj ve görüş açıları nedeniyle kör noktalar oluşabilmektedir.
- (4) Güvenlik kameraları karanlık ortamlarda da kayıt yapabileceği, yüz ve eşkâl belirlemeye yardımcı olacak şekilde yerleştirilmiştir.
- (5) Üniversitemiz Destek İşleri Şube Müdürlüğü güvenlik personelleri, birim ve ana izleme merkezlerinde bulunan kamera izleme noktalarından kampüs içerisindeki anlık görüntüleri izleyerek olaylara anında müdahale edilmesi hususunda gerekli tedbirleri almaktan sorumlu olacaktır.
- (6) Arşiv görüntülerine tarih ve saat girilerek kolayca ulaşılabilmektedir.
- (7) İlgili birim amirlerine anlık görüntü kayıtları ve arşiv izleme yetkileri tanımlanarak kapalı zarf içerisinde (kullanıcı adı, şifre) verilecektir. Ancak sistem üzerinde yaratacağı yük nedeni ile Başkanlık anlık izlenecek olan kamera sayılarında kısıtlama yetkisine sahiptir.
- (8) Sistemde görüntüler (kapasite ölçüsünde) 15 gün süre ile kayıt altına alınmaktadır.
- (9) Emniyet Müdürlüğüne veya Cumhuriyet Savcılığının yazılı talebi ile ana izleme merkezi veya birim izleme merkezindeki kayıtlı görüntüler, Rektörlük Makamının yazılı izni ile verilir.
- (10) Asayiş ve güvenliği ilgilendiren ve delil niteliğinde olan görüntüler Emniyet Müdürlüğü veya Cumhuriyet Savcılığının yazılı isteği ile belirlenen ilgili zaman süresini kapsayacak şekilde CD/DVD ortamında teslim edilen görüntülerin bir kopyası da arşivlenerek 5 (beş) yıl süre ile Destek İşleri Şube Müdürlüğünde saklanır ve sürenin sonunda imha edilir.
- (11) Birim izleme merkezinde kayıtlı görüntülerin güvenli arşivlenmesi ve saklanmasından ilgili birim yöneticisi; ana izleme merkezinde kayıtlı görüntülerin güvenli arşivlenmesi ve saklanması Başkanlık tarafından sağlanacaktır.
- (12) Birim ve ana izleme noktalarında tutulan kayıtların izlenme talepleri, kişinin dilekçesine istinaden ilgili birim amirinin oluşturacağı komisyon ve dilekçe sahibinin katılımı ile görüntü izlenecektir. Ortak alanlardaki arşiv görüntülerinin izlenmesi Destek İşleri Şube Müdürlüğü tarafından oluşturulacak komisyonca izlenecek ve gerekli işlemler yapılacaktır.

Kurum Ağacı ve Kimlik Yönetim Sistemi Kullanım Politikası

Madde 10 - (1) Kamu ve kuruluşlarının KamuNet'e dahil edilmesine ilişkin 2016/28 sayılı Başbakanlık genelgesine istinaden, üniversitemiz birimlerinde görev yapmakta olan akademik ve



BİLGİ İŞLEM DAİRE BAŞKANLIĞI
İNTERNET VE YEREL AĞ SERVİSLERİ
KULLANIM YÖNERGESİ

Doküman No	YÖ-058
İlk Yayın Tarihi	20.04.2017
Revizyon Tarihi	06.06.2018
Revizyon No	01
Sayfa	5 / 7

idari personel ile öğrencilerin kullanmakta olduğu tüm bilişim cihazları (sunucular, bilgisayarlar, yazıcılar, tarayıcılar vb.) kurum ağacı ve kimlik yönetim sistemine dahil olacaktır.

- (2) Üniversitemiz bünyesinde çalışmakta olan veya işe başlayan her personel ile paydaş ve konuklar için kullanıcı hesabı açılacaktır.
- (3) Kullanıcı hesabı açılırken Türkçe karakterler “ç, ş, i, ö, ü, ğ” kullanılmayacaktır.
- (4) Kullanıcı, kendisine verilen “kullanıcı adı” nı ve “şifre” sini bir başkası ile paylaşmaz ve bir başkasına kullandırmaz. Kullanıcı “kullanıcı hesabına” ait geçici şifresini derhal değiştirerek, Madde-15’te yer alan şifre politikasına göre uygun şifresini oluşturacaktır.
- (5) Kullanıcılar Başkanlıkça belirlenecek periyotlarla “kullanıcı şifresini” değiştirmesi gerekir. Kullanıcı şifresini yenilemeyen veya kullanıcı şifresini üst üste birkaç kez hatalı giren kullanıcının hesabı kilitlenerek iletişim ağına bağlantısı kesilir. İlgilinin başvurması halinde tekrar aktif edilir.
- (6) 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.
- (7) İlgili hesabın amacı dışında kullanılması ve bu hesaptan doğabilecek zararların sorumluluğu, hesabı kullanan kullanıcıya aittir.

Ağ ve Sistem Kullanım Politikası

Madde 11 - (1) Tüm kullanıcılar interneti bilinçli bir şekilde kullanmak, başkalarının haklarını ihlal edici ve bilişim sisteminin işleyişini engelleyici, bozucu faaliyetlerde bulunmamakla yükümlüdür.

- (2) Kullanıcılar, kendisine tahsis edilen her türlü bilişim cihazı içerisinde bulundurduğu belge, yazılım gibi her türlü kaynağın içeriğinden sorumludur.
- (3) Başkanlık tarafından kullanıcıların kullanımına sunulan güvenlik programlarının aktif olarak kullanılması zorunludur. Bu husustan kullanıcılar sorumludur.
- (4) Kullanıcılar, yerel ağ üzerinden, iç ağda bulunan sistemler ile dış ağda bulunan sistemlere saldırı niteliğinde ki girişimlerde bulunamazlar.
- (5) Kullanıcılar, kendilerine tahsis edilen bilişim cihazları içerisinde, telif hakları ve lisansları ihlal edici nitelikte yazı, makale, kitap, film, müzik, program vb. materyalleri bulunduramazlar.
- (6) Kullanıcıların kendilerine tahsis edilen bilişim cihazlarının IP numarası, MAC adresi ile BIOS ayarlarını, Başkanlıkça yetkilendirilmiş kişiler dışında ki kullanıcılar değiştiremezler.

Arıza ve Bakım Kullanım Politikası

Madde 12 - (1) Kullanıcılar, kendilerine tahsis edilen bilişim cihazlarındaki arıza veya bakım isteklerini, başkanlığımızın online destek sayfası aracılığı ile iletmek zorundadır.

- (2) Başkanlık, hizmet standartlarında belirtilen süreler içerisinde bakım, onarım veya arızaları giderecektir.
- (3) Kullanıcıların, arızalanan bilişim cihazlarını kendilerinin Başkanlık personeline teslim etmemesi veya almaması durumlarından (çalıntı, kaybolma vb.) Başkanlık personeli sorumlu tutulamaz.
- (4) Kullanıcılar, Başkanlıktan yeniden kurulmasını talep ettikleri bilgisayarların yedeklerinin alınmasından sorumlu olacaktır.



BİLGİ İŞLEM DAİRE BAŞKANLIĞI
İNTERNET VE YEREL AĞ SERVİSLERİ
KULLANIM YÖNERGESİ

Doküman No	YÖ-058
İlk Yayın Tarihi	20.04.2017
Revizyon Tarihi	06.06.2018
Revizyon No	01
Sayfa	6 / 7

Anti-Virüs Kullanım Politikası

Madde 13 - (1) Kullanıcılar, Başkanlık tarafından temin edilen lisanslı anti-virüs programını kullanacaktır.

- (2) Anti-virüs güncellemeleri, sunucu üzerinden otomatik yapılmakta olup, kullanıcılar kendilerine tahsis edilen bilişim cihazlarının güncellemesini kapatmayacaktır.
- (3) Kullanıcılar, kendilerine tahsis edilen bilişim cihazları içerisinde, herhangi bir sebepten dolayı anti-virüs programını sisteminden kaldırmayacak ya da pasif konuma getirmeyecektir.
- (4) Kullanıcılar, kendilerine tahsis edilen bilişim cihazlarını haftalık periyotlarda virüs taramasından geçirecektir.

Elektronik Belge Yönetim Sistemi Kullanım Politikası

Madde 14 - (1) Elektronik Belge Yönetim Sistemi (EBYS), Başkanlığımız bünyesindeki sunucu üzerinde kurularak hizmet vermekte olup, EBYS ile hazırlanan belgeler zaman damgalı olarak imzalanmaktadır.

- (2) Üniversitemizde işe başlayan veya ayrılan personellerin kullanıcı tanımları ya da kullanıcı tanımlarının kapatılması Personel Daire Başkanlığı tarafından yapılır.
- (3) Personel Daire Başkanlığından, Başkanlığımıza elektronik imza temini için gönderilen yazıya istinaden, KamuSM'ne Nitelikli Elektronik Sertifika Başvuru tablosu ile bildirilir. Ardından KamuSM tarafından iletilen formlar ilgili personel tarafından doldurup ıslak imzalı olarak Başkanlığa teslim edilir. İş süreçleri sonunda KamuSM tarafından kişiye özel olarak üretilen Elektronik İmza Sertifikası ve kart okuyucu ilgili personele kurye ile teslim edilir.
- (4) EBYS'ye giriş için, her personel Şifre Politikasına uygun bir şifre belirlemeli ve bilgilerini sistemden kontrol etmelidir.
- (5) Kullanıcılar, imza oluşturma verisini ve güvenli elektronik imza oluşturma aracını başkasına kullandırmaz, bu konuda gerekli tedbirleri alır.
- (6) Kullanıcılar, nitelikli elektronik sertifika kullanım hak ve yükümlülüklerini bir başka kişi veya kuruma devredemez.
- (7) Kullanıcılar, güvenli elektronik imza oluşturma aracı erişim verisini korumakla ilgili her türlü tedbiri almakla yükümlüdür.

Şifre Kullanım Politikası

Madde 15 - (1) Kullanıcı, kurumda kullanılan ve belirli bir şifre ile girilmesi zorunlu olan her türlü uygulama ve bilişim cihazlarına yönelik şifre belirler.

- (2) Kullanıcı şifre belirlerken dikkat edeceği kurallar şunlardır.
 - a) Şifreler en az 8 karakter olmalıdır.
 - b) Şifreler küçük harf, büyük harf, rakam ve simgelerin kullanıldığı karışık yapıda olmalıdır.
 - c) Şifreler en geç altı ayda bir değiştirilmelidir.
- (3) Şifreler herhangi bir kişi ile paylaşılmaz.

Kullanıcıların Sorumlulukları

Madde 16 - (1) Kullanıcı, yukarıda belirtilen hizmetlerden yararlanmaya başladığı andan itibaren bu belgede yer alan maddelere uyacağını kabul eder ve yükümlülüğünü üstlenir.



**BİLGİ İŞLEM DAİRE BAŞKANLIĞI
İNTERNET VE YEREL AĞ SERVİSLERİ
KULLANIM YÖNERGESİ**

Doküman No	YÖ-058
İlk Yayın Tarihi	20.04.2017
Revizyon Tarihi	06.06.2018
Revizyon No	01
Sayfa	7 / 7

Birimlerin Yetki ve Sorumlulukları

Madde 17 - (1) Üniversitemize bağlı bulunan tüm birim (Fakülte Dekanlığı, Yüksekokul, Meslek Yüksekokulu, Enstitü ve Merkez Müdürlükleri ve İdari Yönetim Birimleri) yetkilileri, kendi kullanıcılarına bu yönergeyi duyurmakla yükümlüdür.

Uygulama ve Yaptırım

Madde 18 - (1) Bu yönergede belirtilen maddelerde hükmü geçen davranışlara uyulmadığının Başkanlık veya diğer birimler tarafından tespit edilmesine müteakip aşağıdaki yaptırımlar kullanıcının görev yaptığı birim tarafından uygulanır.

- a) Kullanıcı sözlü veya yazılı olarak uyarılır,
- b) Kullanıcıya verilmiş kaynaklar süreli veya süresiz olarak kullanımından alınır,
- c) Soruşturma ve diğer yasal süreçler başlatılır ve sonuçları uygulanır.

Diğer Hususlar

Madde 19 - (1) Başkanlık, sektörde meydana gelebilecek yasal gelişmeler ve bu Yönerge hükümleri çerçevesinde kullanım kurallarına ilişkin yeni düzenlemeler yapabilir.

Yürürlük

Madde 20 - (1) Bu Yönerge, Kırşehir Ahi Evran Üniversitesi Senatosunca kabul edildiği tarihte yürürlüğe girer ve önceki yönergenin hükümleri uygulanmaz.

Yürütme

Madde 21 - (1) Bu Yönerge hükümlerini Kırşehir Ahi Evran Üniversitesi Rektörlüğü yürütür.

Bu yönerge; Kırşehir Ahi Evran Üniversitesi Senatosunun 06/06/2018 tarih ve 2018/06-01 sayılı kararı ile kabul edilmiştir.