NİĞDE ÖMER HALİSDEMİR ÜNİVERSİTESİ
BİLGİ VE İLETİŞİM GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Bu politikanın amacı, üniversite bilgi ve iletişim varlıklarının gizlilik, bütünlük ve erişilebilirlik temel ilkelerine uyumun sağlanması ile bilgi güvenliği kapsamında kurum itibar ve güvenilirliğini korumak için üst yönetimin yaklaşımını tanımlamak, tüm kullanıcı ve taraflara yapılması ve uyulması gereken ilke ve kuralları bildirmektir.

2. KAPSAM

Bu politika, üniversitenin bilgi ve iletişim varlıklarını kullanan tüm kullanıcıları (personel, öğrenci, mezun, geçici kullanım hakkı verilmiş diğer özel ve tüzel kişiler ile tedarikçi, tedarikçi çalışanları, ziyaretçiler) ve bu varlıklar ile gerçekleştirilen faaliyetleri kapsar.

3. TANIMLAR

BGYS: ISO 27001 Bilgi Güvenliği Yönetim Sistemini,

BİGR: Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) Bilgi ve İletişim Güvenliği Rehberini,

Bütünlük: Bilginin tam ve doğru olma durumunun korunmasını,

Erişilebilirlik: Bilginin yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasını,

Denetim kaydı: Bir bilgi varlığına kimin eriştiğini veya erişmeye çalıştığını ve erişim sağlayan kullanıcının hangi işlemleri gerçekleştirdiğini gösteren kayıtları,

Gizlilik: Bilginin yetkisiz kişilerin erişimine karşı korunmasını,

Gizlilik dereceli bilgi/veri: Bilmesi gereken kişiler dışındakilere açıklanması veya verilmesi, millî güvenlik ve ülke menfaatleri bakımından sakıncalı görülen ve haiz olduğu önem derecelerine göre "ÇOK GİZLİ", "GİZLİ", veya "HİZMETE ÖZEL" şeklinde sınıflandırılan bilgiyi/veriyi,

IP: Internet Protocol/İnternet Protokolünü,

İYS: İstek Yönetim Sistemini,

İz kaydı: Operasyonel bir işlemin başlangıcından bitişine kadar adım adım takip edilmesini sağlayacak kayıtları,

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Kritik bilgi/veri: Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, içeriğinin yetkisiz personel veya kişiler tarafından görülmesi halinde kuruma çok ciddi maddi veya manevi zarar verebilecek her türlü bilgi/veri ve 07/04/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan özel nitelikli kişisel verileri,

Kullanıcı: Üniversitenin bilgi ve iletişim varlıklarını kullanan, personel, öğrenci, mezun, geçici kullanım hakkı verilmiş diğer özel ve tüzel kişiler ile tedarikçi, tedarikçi çalışanı ve ziyaretçileri,

Misafir Öğrenci: Niğde Ömer Halisdemir Üniversitesinin herhangi bir diploma programına kayıtlı olmaksızın, belirli şartlarla ve sınırlı sürelerle Üniversitede ders almalarına izin verilen öğrencileri,

Özel nitelikli kişisel veri: başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olmasına veya ayrımcılığa maruz kalmasına neden olabilecek nitelikteki verileri,

Siber olay: Bilgi ve iletişim varlıklarında bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini; ihlal teşebbüsünde bulunulmasını,

SOME: Siber olaylara müdahale ekibini,

Uygulama yöneticisi birimi: Üniversite uygulamalarının, temini, geliştirilmesi ve güncellenmesi için talepte bulunan, süreci yöneten, uygulama kullanıcılarına ayrıcalıklı rol/yetki tanımlayan birimi,

Uygulama: Üniversite akademik ve idari iş süreçlerini yürütmek amacıyla kullanılan, Bilgi Sistemi/Otomasyon Sistemi/yazılımları,

Taşınabilir cihaz: Taşınabilir bilgisayar, tablet, telefon vb. cihazları,

Taşınabilir ortam: Taşınabilir disk, bellek, optik disk (CD, DVD vb.), hafıza kartları, teyp kartuşları ve benzerlerini,

Ulusal akademik ağ (ULAKNET): Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) tarafından kurulan üniversiteler ve araştırma kurumlarını birbirine bağlayan akademik bilgi ağını,

Üniversite: Niğde Ömer Halisdemir Üniversitesini,

Üniversite bilgi güvenliği yöneticisi: Üniversite bilgi güvenliğinin sağlanmasından ve yönetiminden sorumlu Rektör Yardımcısını,

Varlık: Elektronik ve/veya fiziksel ortamlarda yer alan; iletişim yoluyla aktarılabilen bilgiyi içeren, kurumun iş süreçleri açısından değer taşıyan tüm bilgi ve bilgi işleme olanakları ile bilgiyi kullanan, taşıyan personel ve bilgiyi barındıran fiziksel mekânları,

ifade eder.

10. BİLGİ VE İLETİŞİM VARLIKLARININ KABUL EDİLEBİLİR KULLANIMI POLİTİKASI

10.1 Genel Kullanım Politikası

1. Üniversite, bilgi ve iletişim varlıklarını temel kullanım amaçları (eğitim-öğretim, araştırma-geliştirme, topluma hizmet ve idari/yönetimsel faaliyetleri ile doğrudan ilişkili olan kullanımı) doğrultusunda kullanıcılara sunar, hizmetlerin çalışmasını ve devamlılığını sağlar.

2. Üniversite, temel kullanım amaçları dışında kalan her türlü kullanımı ancak temel kullanımı kısıtlamadığı, kural ve ilkelere aykırı olmadığı sürece kabul eder ve kaynakların etkin kullanılması için gerektiğinde bu tür kullanım için kısıtlamaya gidebilir.

3. Bilgi ve iletişim varlıklarının gizlilik, bütünlük ve erişilebilirliğine ilişkin ihlallerde cezai ve hukuki sorumluluk kullanıcıya aittir. Üniversite bu tür ihlallerin söz konusu olduğu durumları inceler ve bir suç oluştuğundan şüphe duyulursa adli makamlarla işbirliği yapar.

4. Üniversite, bilgi ve iletişim güvenliği gereksinimleri, varlıkların etkin kullanılması ve yasal mevzuata uyum sağlamak amacıyla ilgili sistemlerde iz ve denetim kayıtlarını tutar ve yasal sürelerde saklar. Bu kayıtları istatistik ve siber güvenlik olaylarına müdahale amacıyla kullanır ve analiz eder.

5. Üniversite, bilgi ve iletişim varlıklarının yasal mevzuata, bu politikaya, ilgili kaynağın kullanım kurallarına ve etik değerlere uygun olarak kullanılmadığı durumlarda kullanıcı erişimini engelleyebilir.

6. Üniversite, kullanıcılar ile üçüncü kişi veya kuruluşlar arasında doğabilecek her türlü ihtilafta doğrudan taraf olma hakkını saklı tutar.

7. Bilgi ve iletişim varlıklarının ticari nitelik taşıyan ve gelir teminine yönelik kullanımları söz konusu ise Üniversite Rektörlüğünden izin alınır.

8. Bilgi ve iletişim varlıklarının kullanımında güvenliği bozan girişim bilgilerinin tespiti ve kullanıcı kimliğinin belirlenmesi için yetkili birimlerce gerekli düzenlemeler yapılır.

9. Personel, kurumsal iş süreçlerini yürütmek için Üniversite tarafından sağlanan bilgi ve iletişim varlıklarını kullanır, istisnai durumlarda, personelin bağlı bulunduğu üst yönetici izni ile kişisel bilgi ve iletişim varlıkları kullanılabilir.

10. Kurumsal iş süreçlerini yürütmek için Üniversite tarafından sağlanan cihazların güvenlik ve güncelliğini sağlamak amacıyla Üniversite tarafından merkezî teknik bir altyapı oluşturulabilir.

11. Üniversiteye ait yazılımlar hiçbir şekilde ve sebeple kopyalanamaz, çoğaltılamaz ve üçüncü şahıslarla paylaşılamaz. Lisanslı olmayan yazılımlar kullanılamaz.

10.2 Kullanıcıların Sorumlulukları

1. Üniversite bilgi ve iletişim varlıkları kullanıcıları;
    a) Bilgi ve iletişim varlıklarını yasal mevzuata, bu politikaya, ilgili kaynağın kullanım kurallarına ve etik değerlere uygun olarak kullanmaktan ve gizlilik, bütünlük ve erişilebilirliğini korumaktan,
    b) Bilgi ve iletişim varlıklarına erişim sağlamak amacıyla kendilerine verilen kullanıcı adı ve parolalardan,
    c) Bilgi ve iletişim varlıklarına erişim sağlamak amacıyla, kendilerine verilen kullanıcı bilgileri (kullanıcı yetkisi, kodu, parola, IP adresi vb.) ve Üniversite tarafından belirlenen diğer güvenli oturum açma kullanıcı yöntemleri (e-Devlet, e-imza vb.) ile gerçekleştirdikleri çalışmalar, etkinlikler, bulundurdukları veya yarattıkları bilgi, belge, yazılım gibi her türlü kaynağın içeriğinden,
    ç) Bilgi güvenliği konusunda, ihlal olaylarını ilgili makamlara bildirmekten,
    d) Bilgi ve iletişim varlıklarına ilişkin sorunları belirlemek, çözmek veya esaslara aykırı davranışları tespit etmek amacıyla Üniversite Rektörlüğü ve/veya yetkilendirdiği birimler tarafından talep edilen bilgilerin doğru ve eksiksiz verilmesinden,
    e) Bilgi ve iletişim varlıklarının fiziksel güvenliğini sağlamaktan, güvenlik eksikliğinden kaynaklanacak zararlardan, kullanım kılavuzlarına uygun olarak kullanmaktan ve bilgileri kritik olma düzeyine göre korumak ve yedeklemekten,
    f) Üniversiteye ait olmayan sitelerden indirilen yazılımlardan ve bu yazılımlar nedeniyle oluşacak zararlardan

sorumludur.

2. Kullanıcılar bilgi ve iletişim varlıklarını,
    a) Yetkisiz ve/veya izinsiz olarak üçüncü kişilere/kuruluşlara dağıtamaz, yetkisiz erişim sağlayamaz, diğer kullanıcıların kullanım hakkını engelleyici faaliyetlerde bulunamaz, kaynaklara zarar veremez, kaynakların güvenliğini tehdit etmek amacıyla kullanamaz.
    b) Kişilerin ve kurumların fikri mülkiyet ve kişisel haklarını ihlal, veri ve bilgilerini tahrip, iftira ve karalama, kişi ve kurumların çalışmalarını bozma biçiminde kullanamaz, üzerinde bu nitelikte materyal üretemez ve barındıramaz.

10.3 Parola Güvenliği

10.3.1 Genel Parola Kuralları

1. Parola, bilgi güvenliğinin sağlanması açısından kritik bir öneme sahip olup varlıkların yetkisiz erişimlerinden korunması açısından kullanıcı hesaplarında en önemli güvenlik katmanını teşkil eder.

2. Zayıf seçilmiş bir parola tüm altyapıyı, uygulamaları ve verileri riske atabilir. Uzaktan erişenler dâhil tüm kullanıcılar parola kurallarına uymak zorundadır.

3. Parola kişiye özel ve gizli bilgi olarak değerlendirilmelidir. İşin sürdürülmesi amacıyla bile olsa kimseyle paylaşılamaz. Parolanın güvenliği kullanıcının sorumluluğundadır.

4. Parola, kâğıt ya da elektronik herhangi bir ortamda açıkça yazılmış olarak bulundurulmaz, yazılı bulundurulması gerektiğinde saklanan ortamın güvenliği sağlanır.

5. Bütün seviyelerde kullanılan parolalar yılda en az 1 (bir) kez değiştirilir. Uygulanabilir durumlarda parolanın değişimi için otomatik hatırlatma yapılır.

6. Kullanıcılar, parola belirlerken başkaları tarafından tahmin edilmesi kolay olan aile/arkadaş/sevilen yer/yemek/hayvan/sanatçı isimleri, klavye sıralı harfler, sıralı sayılar, doğum tarihi/yeri, adres veya telefon bilgisi içermemesine özen gösterir.

7. Üniversite sistem ve uygulamalarında kullanılan parolalar, Üniversiteye ait olmayan sistem ve uygulamalarda kullanılamaz. Farklı sistemlerde farklı parola kullanılması olası riskleri azaltır.

8. Kullanıcı, şüpheli bir durumda parolasını mutlaka değiştirmelidir.

9. Üniversitenin sistem ve uygulamalarında parola ölçütü olarak asgari 1 (bir) adet büyük harf, 1 (bir) adet küçük harf, 1 (bir) adet özel karakter, 1 (bir) adet rakam içerir ve parola uzunluğu 8 (sekiz) adet karakterden daha kısa olamaz.

10.3.2 Uygulamalarda Parola Tasarımı ve Saklanması

1. Kullanıcı, Üniversite uygulamalarında kendisine sağlanan bilgilerle ilk oturum açtığında parolasını değiştirir.

2. Uygulamalarda parola ilk kez tanımlanırken veya değiştirilirken parola iki kere girilir, yazılan bilgiler başkaları tarafından görülmemesi için maskelenir.

3. Uygulamalarda parola değiştirme işlemlerinde kullanıcının mevcut parolası istenir.

4. Uygulamalarda izin verilen hatalı giriş sayısı en fazla 20 (yirmi)'dir. Bu sayıdan fazla hatalı girişlerde kullanıcı hesabı kilitlenir, kilitlenen hesaplar belirli bir süre sonra ya da kullanıcı tarafından gerçekleştirilecek parola sıfırlama ve doğrulama yöntemleri ile etkinleştirilir.

5. Uygulama veya hizmetlerin gereksinimlerine göre sınırlı süreli parola tanımlanabilir.

6. Unutulan parola ve parola sıfırlama işleminde farklı doğrulama yöntemleri (e-Devlet, SMS, e-posta, diğer sistemlere erişim vb.) kullanılır.

7. Uygulamalar arasında parola iletimi yapılıyorsa tüm bağlantılar uygun güvenlik metoduyla (https, ssh, ssl, tls vs) korunur.

8. Uygulama erişimlerinde başarılı veya başarısız kullanıcı adı/parola girişimleri kayıt altına alınır.

9. Kullanıcı parolası, uygulama ve hizmetlerde açık parola olarak değil, uygun metotla şifrelenmiş şekilde saklanır.

10.4 Tehdit ve Zafiyet Yönetimi

10.4.1 Zafiyet ve yama yönetimi

1. Bilgi ve iletişim varlıklarına ait tüm yazılımların, mevcut iş gereksinimlerini karşılayacak ve yazılım üreticisi tarafından sağlanan en kararlı ve güncel güvenlik sürümleri ile çalışması sağlanır.

2. Üniversite, ağ, sistem uygulama altyapısında oluşacak zafiyetleri en aza indirmek amacıyla saldırı tespit ve önleme, web uygulama, web içerik ve URL filtreleme ile e-posta filtreleme gibi teknolojik altyapılar kullanır.

3. Ağ, sistem uygulama altyapısında zafiyet tespit edilen IP/site ve kullanıcılar kara listeye alınır.

4. Üniversite, kara liste uygulaması için ulusal ve uluslararası kabul görmüş kara liste veri tabanlarını kullanabilir ve kara listedeki sitelere erişimi engelleyebilir.

5. Üniversite ağında daha fazla güvenlik gerektiren sistemler/sunucular ayrı bir ağda tutulur.

6. Üniversite bilişim altyapısında yer alan ağ ve sistemler ile kritik veri işleyen uygulamalara güvenlik açıklarının zamanında tespit edilmesi için yılda en az 1 (bir) defa teknik açıklık testleri yapılmalıdır. Bu süreç Bilgi İşlem Daire Başkanlığı tarafından yürütülür.

7. Üniversite kamera altyapısında bulunan cihaz ve uygulamaların teknik açıklık, analiz ve uygulamaları Yapı İşleri ve Teknik Daire Başkanlığınca yürütülür.

8. Birimler tarafından kullanılan ve Üniversite ağına dahil edilen cihazların (laboratuvarda kullanılan cihazlar, alarm cihazları gibi IoT cihazlar) güncelleme ve yama işlemleri ilgili birimler tarafından izlenir ve yürütülür.

9. Üniversite kaynakları ile geliştirilen uygulamalara ilişkin güncellemeler ve yamalar Bilgi İşlem Daire Başkanlığınca gerçekleştirilir ve yürütülür.

10. Tedarikçiler tarafından geliştirilen uygulamalarda güncelleme ve yamalar ilgili birimin onayından sonra tedarikçi tarafından gerçekleştirilir. Süreci ilgili birim izler ve kayıt altına alır.

11. Bilgisayar ve taşınabilir cihazlar üzerindeki işletim sistemi ve uygulamaların yüklenmesi ve güncellenmesi kullanıcının sorumluluğundadır.

12. Güncelleme ve yamalar sadece üretici kaynaklarından temin edilir.

10.4.2 Zararlı Yazılımlara Karşı Korunma

1. Üniversite, zararlı yazılımların kullanıcı cihazları ve altyapı bileşenleri üzerinde çalışmasını, kaydedilmesini ve aktarılmasını engelleyecek güvenlik önlemleri için çalışmalar yapar.

2. Üniversite, zararlı yazılımların kontrolü amacıyla lisanslı zararlı yazılımdan korunma uygulamaları (antivirüs) temin eder.

3. Antivirüs yazılımı Üniversite sunucularında merkezi olarak yönetilir, yazılımda en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanır. Tespit edilen zararlı yazılımlar ve kullanıcı bilgileri kayıt altına alınır.

4. Üniversiteye ait tüm bilgisayar ve taşınabilir cihazlara lisanslı antivirüs uygulaması kullanıcı tarafından kurulur ve güncel tutulması sağlanır. Kullanıcı antivirüs yazılımını devre dışı bırakamaz.

5. Üniversite ağını kullanan ve uzak erişimine izin verilen kullanıcılara ait cihazlarda da antivirüs uygulaması kurulu, güncel ve etkin olmalıdır.

6. Kullanıcılar tarafından virüsün varlığından şüphelenildiğinde cihazın ağ bağlantısı kesilir, bilgi güvenliği ihlal olayı söz konusu ise durum birim yöneticisine iletilir.

7. Güvenilmeyen kaynaklardan alınan dosyalar, diğer dosyaların bulunduğu ortama aktarılmadan zararlı yazılım taramasından geçirilir.

8. Taşınabilir ortamlar, kullanılmadan önce zararlı yazılım taramasından geçirilir.

9. Kullanıcılar, bilgi ve iletişim varlıklarının normal işleyişine zarar verebilecek uygulamaları ağ üzerinden ya da farklı yöntemlerle yayamaz.

10. Üniversite, zararlı yazılım tespit edilen cihazların ağ erişimini engelleyebilir.

10.5 e-Posta Kullanımı

10.5.1 Genel Kurallar

1. Üniversite, personel, öğrenci, mezun ve birimler için kurumsal elektronik posta (e-posta) hesabı sağlar.

2. Kurumsal e-posta hesabı, personel için göreve başlama sırasında Personel Daire Başkanlığı tarafından oluşturulur, e-posta hesap adı personel ad ve/veya soyadını ya da bunların kısaltmalarını içerecek şekilde sistem tarafından oluşturulan seçenekler arasından personel tarafından seçilir.

3. Üniversitede kayıtlı öğrenciler isterse Öğrenci Bilgi Sistemi üzerinden kurumsal e-posta hesabı oluşturabilirler. e-Posta hesap adı öğrencinin adını ve soyadını içerecek şekilde sistem tarafından oluşturulur.

4. Birimler için kurumsal e-posta hesabı, ilgili birimin talebi üzerine oluşturulur ve birimde görevlendirilen personel tarafından yönetilir. Birim e-posta hesabını yöneten personel değiştiğinde e-posta hesabı için parola güncellenir.

5. Birim e-posta hesaplarına ilişkin hesap adı, birim/bölüm/proje, yönetici vb. bilgileri içeren envanter kaydı ilgili birimlerce tutulur. İlgili birimler, envanter kayıtlarını yılda en az 1 (bir) kez kontrol eder ve kullanılmayan hesapların kapatılmasını sağlar.

6. e-Posta kullanıcıları, kendilerine ait kurumsal e-posta hesabından gönderilen e-postalardan doğacak hukuki sonuç ve işlemlerden sorumludur.

7. Üniversiteden ayrılan personel ve öğrencinin kurumsal e-posta hesabı kapatılır. Mezunlar isterse öğrenci oldukları dönemde kullandıkları kurumsal e-posta hesaplarının aktif edilmesini Öğrenci Bilgi Sistemi üzerinden talep edebilirler.

8. Üniversiteden ayrılan personel ve öğrencinin kurumsal e-posta hesabı 5 (beş) yılın sonunda silinir.

9. Bilgi İşlem Daire Başkanlığı, e-posta sistem güvenliğini sağlamak amacıyla izleme, istatistik yapma, kuralları belirleme ve gerektiğinde kullanıcı e-posta erişimini engelleme yetkisine sahiptir.

10.5.2 Kurumsal e-posta kullanımı

1. Kurumsal e-posta hesabı, kötü amaçlar ve doğrudan ya da dolaylı olarak ticari ve kar amaçlı olarak kullanılamaz. Kurum içi ve dışı herhangi bir kişi ve grubu küçük düşürücü, hakaret edici, uygun olmayan, fikri mülkiyet haklarını ihlal eden ve zarar veren nitelikte e-posta mesajları gönderilemez.

2. Kullanıcılar, e-posta adresinin "kimden*"* bölümüne başka bir kullanıcıya ait e-posta adresini yazamaz.

3. e-Postaya eklenecek dosya uzantıları, Üniversite tarafından yasaklanan uzantılar olamaz, zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda dosyalar sıkıştırma yazılımı ile mesaj olarak gönderilir.

4. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar, zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya, virüs, oltalama e-postaları açılmamalı, alındığında silinmeli ve başkalarına iletilmemelidir.

5. e-Posta ile gönderilmek istenen ek dosyanın maksimum boyutu 20 (yirmi) MB olmalı, daha büyük boyutlu ekler için dosya paylaşım sistemi kullanılmalıdır.

10.5.3 Üniversite iş süreçlerinde e-posta hesabının kullanılması

1. Üniversite adına yapılan tüm e-posta haberleşmeleri, kurumsal e-posta hesapları yoluyla yapılır, kişisel e-posta hesapları kurumla ilgili haberleşmelerde kullanılmaz.

2. Gizlilik dereceli ve kritik veri içeren bilgi ve belgeler, açık metin ya da ek olarak e-posta ile gönderilmez, zorunlu durumlarda ise içerik şifrelenir.

3. e-Posta gönderirken alıcının doğru seçildiğinden emin olunur, mesajların yetkisiz kişiler tarafından okunması engellenir ve kuruma özel e-postalar kurum dışındaki üçüncü şahıslar ile paylaşılamaz.

4. e-Posta gönderilirken "konu" alanı boş olarak gönderilemez, içerikte resmi bir dil kullanılır, yazım kurallarına uyulur, tamamı büyük harften oluşan cümleler yazılmaz, farklı yazı formatları kullanılmaz, ek dosya adları düzenlenir, gönderen kişi, birim ve ünvan bilgileri belirtilir.

5. Toplu e-posta gönderimlerinde alıcıların diğer kişilere ait e-posta adreslerini görmemesi gerekliyse Gizli Karbon Kopya (GKK) seçenekleri kullanılır.

10.6 Ağ ve İnternet Kullanımı

1. Üniversite; personel, öğrenci, misafir personel/misafir öğrenci, eduroam kullanıcıları ile Rektörlükçe izin verilen etkinlik katılımcılarına ağ ve internet hizmeti sağlar.

2. Kullanıcılar, sahip oldukları cihazları kişisel kullanımları için üniversite ağına dâhil edip internet altyapısını kullanabilir.

3. Üniversite ağ ve internet altyapısı akademik, idari, eğitim, öğretim ve araştırma iş süreçlerinin geliştirilmesi ve iyileştirilmesine hizmet eder. Ayrıca Üniversite, kullanıcıların kişisel gelişimine katkıda bulunmak amacıyla internet kullanımını kabul eder.

4. Üniversite, kablolu ya da kablosuz ağ altyapısında kullanıcı kimlik bilgilerini doğrulamak için kullanıcı adı, parola, cihaz donanım adres bilgisinin kaydedilmesi, SMS, e-Devlet doğrulama gibi yöntemler kullanabilir. Eduroam kullanıcıları kablosuz ağ altyapısından kendi kurumlarına ait kullanıcı adı ve parola ile yararlanabilirler.

5. Üniversite ağında IP adresi dağıtımı, merkezî olarak sağlanır. Kullanıcılar IP adresi dağıtımı yapamaz ve cihazlarına el ile IP adresi tanımlayamaz.

6. Sabit IP adresi ihtiyacı olan durumlar için ilgili birimler Bilgi İşlem Daire Başkanlığı ile iletişime geçer.

7. Bilginin gizlilik, bütünlük ve erişilebilirliğini tehdit edecek veri (sistem kullanım parolası, güvenlik parametreleri vb.) ağ ve internet üzerinden uygun güvenlik metoduyla şifrelenerek gönderilir.

8. Kullanıcılar internet kullanımında ULAKNET Kullanım Politikasına uyar.

9. Kullanıcılar, ağ ve internet üzerinde servis kalitesini etkileyecek, bozacak, karışıklık yaratacak trafik düzenlemeleri oluşturamaz, şahsi kazanç ve kar amacı ile kullanamaz.

10. Kullanıcılar, kurumsal ağda bulunan diğer kullanıcıların kişilik haklarını ve kişisel bilgilerinin güvenliğini tehdit edici eylemlerde bulunamaz, Üniversite ağ kaynaklarının üniversite dışından kullanılmasına sebep olabilecek ya da üniversite dışındaki kişi ya da bilgisayarların kendilerini üniversite içindeymiş gibi tanıtmalarını sağlayan ortamlar kullanamaz ve bu ortamları sağlayamaz.

11. Kurumsal ağ ve internet üzerinden birincil kullanım amaçlarına uygun olmayan, güvenli olmadığı bilinen ve genel ahlak anlayışına aykırı sitelere girilemez, Üniversite tarafından onaylanmamış yazılımlar indirilemez, 5846 sayılı Fikir ve Sanat Eserleri Kanunu uyarınca telife sahip dosyalar kopyalanamaz ve dağıtımı yapılamaz.

12. Üniversite; yasal gereklilikler, güvenlik ve kapasite yönetimi nedeniyle ağ ve internet kullanımında filtreleme yapabilir.

13. Üniversite ağ altyapısından gerçekleştirilen internet erişimleri Üniversite tarafından denetlenir, yasa gereği kayıt altına alınır ve saklanır.

14. Bilgi İşlem Daire Başkanlığı; ağ güvenliği, kapasite yönetimi ve iş kaybının önlenmesi amacı ile ağ ve internet kullanımını gözlemleme, istatistik yapma, kurallar belirleme ve gerektiğinde kullanıcı ağ erişimini engelleme yetkisine sahiptir.

10.7 Sosyal Medya Kullanımı

10.7.1 Kurumsal Sosyal Medya Hesapları Yönetimi

1. Üniversite kurumsal kimliğini temsil etmek, her türlü etkinlik ve çalışmayı kamuoyu nezdinde daha görünür kılmak ve paydaşlarla etkileşimi artırmak amacıyla Rektörlük tarafından uygun görülen sosyal medya platformlarında kurumsal sosyal medya hesapları oluşturulabilir.

2. Kurumsal sosyal medya hesabı oluşturacak birimler, Kurumsal İletişim Koordinatörlüğüne bilgi verir.

3. Sosyal medya platformu, hesap adı, kullanıcı adı, hesap yöneticisi vb. bilgileri içeren kurumsal sosyal medya hesap envanterleri ilgili birimler ve Kurumsal İletişim Koordinatörlüğü tarafından takip edilir.

4. Öğrenci kulüpleri için oluşturulacak sosyal medya hesapları için Sağlık Kültür ve Spor Daire Başkanlığından izin alınır. Sosyal medya platformu, hesap adı, kullanıcı adı, hesap yöneticisi vb. bilgileri içeren kulüp sosyal medya hesabı envanteri Sağlık Kültür ve Spor Daire Başkanlığı tarafından takip edilir.

5. Kurumsal sosyal medya hesapları oluşturulurken @ohu.edu.tr uzantılı kurumsal e-posta hesapları kullanılır. Hesap profilinde kullanılacak isim, ilgili birimin/kulübün resmî adını taşır.

6. Sosyal medya hesaplarına giriş için kullanılan parolalar ile Üniversite uygulamalarında kullanılan parolalar farklı olmalıdır.

7. Kurumsal sosyal medya hesabını yönetmek, içerikleri güncellemek ve sorulan sorulara yanıt vermek üzere ilgili birim tarafından sosyal medya yöneticisi görevlendirilir.

8. Kurumsal sosyal medya hesaplarından sadece üst makamlar ile diğer kamu kurumlarının sosyal medya hesapları takip edilebilir; siyasi parti, dernek, oluşum ve diğer tüzel kimlik taşıyan kurum, kuruluş ve kişisel hesapların takibi yapılamaz.

9. Sosyal medya yöneticileri, paylaştıkları her bilgi ve verinin içeriğinden sorumludur ve hesapların parolasını kimseyle paylaşamaz. Kurumsal sosyal medya hesapları yönetiminde içerik, paylaşım ve yorumlara ilişkin sorun oluşması durumunda, ilgili birim yöneticisi ve Kurumsal İletişim Koordinatörlüğü bilgilendirilir.

10. Kurumsal sosyal medya hesapları üzerinden yapılan tüm paylaşımlar ilgili birim tarafından kayıt altına alınır.

11. Kurumsal sosyal medya hesapları üzerinden resmi açıklamalar dışında doğruluğu teyit edilmemiş bilgiler paylaşılamaz.

12. Üniversiteye ait hiçbir gizlilik dereceli bilgi/belge ve yazı sosyal medyada paylaşılamaz, paylaşımlarda kişisel verilerin korunmasına ve özel yaşamın mahremiyetine önem verilir.

13. Kurumsal sosyal medya hesaplarında kişisel bilgiler paylaşılmamalı, yayınlanan içerikler, Üniversite kimliğine, telif haklarına ve etik kurallara uygun olmalıdır.

14. Sosyal medyada kullanılan kelimelere ve dile dikkat edilir; görevin gerektirdiği ciddiyet ve düzey korunur; ayrımcı, rahatsız edici, ırkçı, cinsel, etnik, dini ya da fiziksel saldırı ve aşağılama niteliğinde ifadeler paylaşılamaz ve bu tür durumlara aracı olunamaz.

10.7.2 Kişisel Sosyal Medya Hesapları

1. Sosyal medyada Niğde Ömer Halisdemir Üniversitesi adıyla açılan her sayfa/hesap Niğde Ömer Halisdemir Üniversitesi resmi alanı gibi düşünülebilir ve paylaşılan tüm içerik Üniversite ile bağdaştırılabilir. Bu nedenle, yanlış bir marka algısı yaratmamak adına personel, öğrenci, tedarikçi, diğer özel ve tüzel kişiler Üniversite ismi ve logosunu kullanarak sayfa/hesap oluşturamaz.

2. Personelin Üniversite içindeki görevi, Üniversite adına açıklamada bulunmak değilse, sosyal medyada ifade edilen görüş ve fikirlerin aynı zamanda Üniversite görüşlerini temsil ettiği izlenimini vermemelidir.

3. Personel, tedarikçiler ve tedarikçi çalışanları Üniversite adını içeren ya da Üniversite ile ilişkilendirilebilecek sosyal medya kullanımlarında; Üniversiteye ait hiçbir gizlilik dereceli bilgi ve belgeyi, onaylanmamış gelişmeyi, müziği, videoyu, yazıları ve fotoğrafları Üniversitenin izni olmadan paylaşamaz.

4. Personel ve öğrencilerin kişisel sosyal medya hesap içerikleri ve paylaşımları Üniversitenin sorumluluğunda değildir.

5. Kişisel sosyal medya hesaplarından yapılan paylaşımlarda Üniversite logosu ya da görüntüsü kullanılamaz.

6. Üniversite içi bilgiler kişisel hesaplardan sosyal medyada paylaşılamaz.

7. Üniversiteden hizmet almış tüm özel ve tüzel kişilikler ile Üniversite personelini ilgilendiren sosyal medya paylaşımları, ilgili kişi ve Üniversitenin bilgisi ve izni olmaksızın yapılamaz.

10.8 Taşınabilir Cihaz ve Ortam Kullanımı

10.8.1 Taşınabilir Bilgisayar Güvenliği

1. Taşınabilir bilgisayar, Üniversite bilgi ve verisini kurum dışına taşıma imkânı sağladığından ve önemli açıklar içerdiğinden, bunun getirdiği riskler dikkate alınır.

2. Taşınabilir bilgisayarda gizlilik dereceli ve kritik veri içeren bilgi ve belgeler saklanmaz, saklama zorunluluğu var ise şifreli olarak saklanır. Üniversiteye ait diğer bilgi ve belgeler ise sadece iş gereksinimi ise tutulur, çalınma ve kaybolma riskine karşı disk şifreleme uygulanır.

3. Kişisel taşınabilir bilgisayarlarda Üniversiteye ait bilgi ve veri tutulmaz.

4. Taşınabilir bilgisayar envanteri birimler tarafından oluşturulur.

5. Taşınabilir bilgisayar, çalınma riskine karşı gözetimsiz bırakılmaz ve fiziksel güvenliği sağlanır. Cihazın korunmasından kullanıcı personel sorumludur.

6. Üniversiteye ait taşınabilir bilgisayar ile Üniversite bilgi ve verisine erişen kişisel bilgisayarlara erişim için Bilgi ve İletişim Varlıklarının Kabul Edilebilir Kullanımı Politikasında belirtilen parola kurallarına uygun bir PIN ya da parola oluşturulur, cihaz kullanılmadığında parolanın otomatik olarak devreye girmesi sağlanır.

7. Taşınabilir bilgisayar Üniversite kaynaklarına uzaktan erişim amacıyla kullanılıyorsa erişim için kullanılan kullanıcı adı ve parola bilgileri kaydedilmez.

8. Üniversiteye ait taşınabilir bilgisayara, Üniversite lisanslı yazılımları dışında yazılımlar kurulmaz.

9. Taşınabilir bilgisayarda işletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması ve antivirüs programlarının kurulu, güncel ve etkin olması sağlanır, güvenlik duvarı kurulur ve aktif edilir.

10. Taşınabilir bilgisayarda bulunan Üniversite bilgi ve verisinin yedekleri alınır ve güncel bir kopyası farklı bir ortamda saklanır.

11. Taşınabilir bilgisayarda kullanımda olmayan kablosuz teknolojiler (wifi, hotspot, airdrop vb.) kapalı tutulur, güvensiz kablosuz ağlara bağlanılmaz, halka açık şarj istasyonlarında şarj edilmez.

12. Taşınabilir bilgisayar, onarım/tadilat için üçüncü kişilere (yetkili servis vb.) verilecekse fabrika ayarlarına döndürülür ve içindeki kurumsal bilgi ve veri güvenli yöntemler kullanılarak silinir.

13. Taşınabilir bilgisayar, elden çıkarılmadan veya yeniden kullanılmadan önce depolama ortamı içeren tüm parçaları, üzerinde herhangi bir kritik bilgi, veri ve/veya lisanslı yazılım varsa kaldırılır veya güvenli şekilde üzerine yazılmasını sağlamak için kontrol edilir.

14. Taşınabilir bilgisayarların depolama ortamı içeren tüm parçaları, bilgi ve veri sızıntılarını önlemek amacıyla Üniversite imha politikalarına uygun ve güvenli olarak imha edilir.

10.8.2 Akıllı Telefon ve Tablet Kullanımı

1. Akıllı telefon ve tablet, Üniversite bilgi ve verisini kurum dışına taşıma imkânı sağladığından önemli açıklar içerir, bunun getirdiği riskler dikkate alınır.

2. Üniversite tarafından sağlananlar dışında kişisel akıllı telefon ve tabletlerde Üniversite bilgi ve verisi saklanmaz.

3. Akıllı telefon ve tabletlerde gizlilik dereceli ve kritik bilgi/veri içeren bilgi ve belgeler tutulmaz, saklama zorunluluğu var ise şifreli olarak saklanır. Üniversiteye ait diğer bilgi ve belgeler ise sadece iş gereksinimi için tutulur.

4. Üniversite bilgi ve verisine erişirken, Root ve jailbreak yapılmış cihazlar kullanılmaz.

5. Akıllı telefon ve tablet envanteri birimler tarafından oluşturulur.

6. Akıllı telefon ve tablet, çalınma riskine karşı gözetimsiz bırakılmaz ve fiziksel güvenliği sağlanır. Cihazın korunmasından kullanıcı personel sorumludur. Akıllı telefon ve tablet, çalınma ve kaybolma riskine karşı uzaktan fabrika ayarlarına döndürülebilecek şekilde ayarlanır.

7. Akıllı telefon ve tablette bulunan Üniversite bilgi ve verisinin yedeği alınır ve güncel bir kopyası farklı bir ortamda saklanır.

8. Üniversiteye ait Akıllı telefon ve tablete erişim için Bilgi ve İletişim Varlıklarının Kabul Edilebilir Kullanımı Politikasında belirtilen parola kurallarına uygun bir PIN ya da parola oluşturulur, cihaz kullanılmadığında parolanın otomatik olarak devreye girmesi sağlanır ve 20 (yirmi) hatalı denemeden sonra cihaz fabrika ayarlarına dönecek şekilde ayarlanır.

9. Akıllı telefon ve tablet Üniversite kaynaklarına uzaktan erişim amacıyla kullanılıyorsa erişim için kullanılan kullanıcı adı ve parola bilgileri kaydedilmez.

10. Üniversiteye ait akıllı telefon ve tablete, Üniversite lisanslı yazılımları dışında yazılımlar kurulmaz, güvenilir kaynaklardan sağlanan mobil uygulamalar kurulur.

11. Akıllı telefon ve tablette, işletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması ve antivirüs programlarının kurulu, güncel ve etkin olması sağlanır.

12. Güncelleme almayan akıllı telefon ve tablette Üniversite bilgi ve verisi saklanmaz ve Üniversite verisine erişilmez.

13. Akıllı telefon ve tablette, kullanımda olmayan kablosuz teknolojileri (wifi, hotspot, airdrop vb.) kapalı tutulur, güvensiz kablosuz ağlara bağlanılmaz ve halka açık yerlerde şarj edilmez.

14. Akıllı telefon ve tablet onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecekse fabrika ayarlarına döndürülür ve içindeki kurumsal bilgi ve veri güvenli yöntemler kullanılarak silinir.

15. Akıllı telefon ve tablet, elden çıkarılmadan veya yeniden kullanılmadan önce depolama ortamı içeren tüm parçaları, herhangi bir kritik bilgi/veri ve/veya lisanslı yazılım varsa kaldırılmasını veya güvenli şekilde üzerine yazılmasını sağlamak için kontrol edilir.

16. Üniversite bilgi ve verisine erişen kişisel akıllı telefon ve tablet fabrika ayarlarına döndürülmeden önce üçüncü kişilere satılmaz.

17. Akıllı telefon ve tablet, veri sızıntılarını önlemek amacıyla Üniversite imha politikalarına uygun ve güvenli olarak imha edilir.

10.8.3 Taşınabilir Ortam Kullanımı

1. Taşınabilir ortamlar, Üniversite bilgi ve verisini kurum dışına taşıma imkânı sağladıklarından önemli açıklar içerir, bunun getirdiği riskler dikkate alınır.

2. Üniversite tarafından sağlananlar dışında kişisel taşınabilir ortamlarda Üniversite bilgi ve verisi saklanmaz.

3. Üniversiteye ait taşınabilir ortamlar listesi ve kimler tarafından kullanıldığı ilgili birimler tarafından kayıt altına alınır.

4. Gizlilik dereceli ve kritik veri içeren bilgi ve belgeler taşınabilir ortamlarda tutulmaz. Özellikle bu tür ortamlarda saklama veya taşıma zorunluluğu var ise şifreli olarak saklanır.

5. Üniversite bilgi ve verisi barındıran taşınabilir ortamlar kurum dışına çıkarılacak ise ilgili birim yöneticisinden izin alınır.

6. Üniversite bilgi ve verisi barındıran taşınabilir ortamlar Üniversiteye ait cihazlar dışında kullanılmaz.

7. Tüm taşınabilir ortamlar, olumsuz fiziksel etkilere karşı üretici tarafından tavsiye edilen saklama ve kullanım koşullarına uygun olarak kullanılır.

8. Bir bilgi sadece taşınabilir ortamda saklanıyorsa, bozulma/kaybolma gibi ihtimallere karşı bir başka ortamda daha yedeklenir.

9. Taşınabilir ortamlar elden çıkarılmadan veya yeniden kullanılmadan önce içindeki kurumsal bilgi ve veri güvenli yöntemler kullanılarak silinir.

10. Taşınabilir ortamlar, veri sızıntılarını önlemek amacıyla Üniversite imha politikalarına uygun ve güvenli olarak imha edilir.