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.

9. ERİŞİM YÖNETİMİ POLİTİKASI

9.1 Erişim Kontrolü

1. Bilgi güvenliğini sağlamanın en temel yolu, bilgi varlığına yetkisiz erişimleri engellemek, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak, bununla ilgili önlemleri almak ve yetkisi olan kişilerin erişimlerini de ihtiyaca göre karşılamaktır.

2. Erişim kontrolünün amacı, bilgi ve iletişim varlıklarına yapılacak olan erişimlerin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak erişmesini sağlayacak bir sistemin kurulmasıdır.

3. Erişim kontrollerinde yasal gereksinimler ile kurum ihtiyaçları göz önünde bulundurulur ve varlık sınıflandırmasına uygun yetkilendirmeler yapılır.

4. Herhangi bir gizliliği olmayan, herkesin erişimine açık olan (tasnif dışı) bilgiler için özel bir erişim kontrol tedbiri alınmasına gerek yoktur. Bu tür bilgiler, internet ve duyuru panosu gibi ortamlarda yayımlanabilir.

5. Bilgi ve iletişim varlıklarının kritiklik seviyesi ve bilginin gizlilik derecesi yükseldikçe uygulanacak olan erişim kontrol politikalarının sıkılaştırılması gerekir ve bu varlıklara ve bilgiye kimin hangi yetki ile erişeceği kararı birim yöneticisi tarafından verilir.

6. Bilgi ve iletişim varlıklarına fiziksel olarak yapılacak erişimler için Fiziksel ve Çevresel Güvenlik Politikasında belirtilen önlemler alınır.

7. Sistem ve uygulamalar üzerinden bilgiye/veriye erişimde kullanıcı kimlikleri doğrulanır, görev ve süreçlerini yönetecek kadar yetki istenir/verilir.

9.2 Kullanıcı Erişim Yönetimi ve Kimlik Doğrulama

1. Üniversitede kullanılan sistemlere ve uygulamalara erişim için kimlik doğrulama mekanizmaları kullanılır.

2. Üniversite uygulamalarına erişim sağlanabilmesi için kullanıcıları benzersiz olarak tanımlayan bir kullanıcı hesabı (T.C. kimlik numarası, öğrenci numarası, sicil numarası, e-posta vb.) oluşturulur ve uygulamalara erişim kullanıcı rol/yetki düzeyinde sağlanır.

3. Üniversite uygulamalarına, oluşturulan kullanıcı adı/parola ya da belirlenen başka bir güvenli oturum açma yöntemiyle (e-devlet, e-imza vb.) erişim sağlanır.

4. Üniversite uygulamalarında oturum açma mekanizmasında güvenliği artırmak amacıyla ek güvenlik önlemleri alınır ve doğrulama yöntemleri (SMS, e-posta vb.) kullanılır.

5. Üniversite uygulamaları için kullanıcı hesabı oluşturma sürecinde, ilk parola kullanıcıya güvenli yollardan iletilir ya da farklı doğrulama yöntemleri (e-Devlet, SMS vb.) ile kullanıcının sisteme erişip kendi parolasını oluşturması sağlanır.

6. Kimlik doğrulama merkezî olarak yapılır. Merkezî kimlik yönetim ve doğrulama sisteminin kullanılamadığı durumlarda, risk analizi çalışması doğrultusunda telafi edici önlemler alınır.

7. Tüm kimlik doğrulama bilgileri güçlü kriptografik algoritmalar kullanılarak saklanır ve şifreli kanallar kullanılarak iletilir.

8. Gizlilik dereceli bilgi ve verinin saklandığı/işlendiği sistemler üzerinde sistem yönetimi amacıyla açılan oturumlar sırasında gerçekleştirilen faaliyetler kayıt altına alınır.

9. Kullanıcı hesaplarına ait parolalar belirlenirken Bilgi ve İletişim Varlıklarının Kabul Edilebilir Kullanımı Politikasında belirtilen parola kuralları uygulanır.

10. İşlem yapılmayan oturumlar belirli bir süre sonra sonlandırılır, tüm başarılı ve başarısız kimlik doğrulama girişimleri için özet veri içerecek şekilde iz kaydı oluşturulur.

11. Üniversite bilgi ve iletişim varlıklarının yönetiminde, varsayılan kullanıcı adı ve/veya parola kullanılmaz.

12. Sistem yöneticilerine, yüksek haklar gerektiren işlemleri yapmaları için ayrı bir hesap oluşturulur.

9.3 Kullanıcı Kaydetme, Silme ve Erişime İzin Verme, Düzenleme ve Kaldırma

1. Üniversite uygulamalarında, Kullanıcı hesap işlemleri (açma, kapama, değişiklik) ve erişim talepleri tanımlı bir süreç ile takip edilir ve bu süreçler Bilgi İşlem Daire Başkanlığı web sayfasında yayınlanır, talep ve işlem süreçleri kayıt altına alınır.

2. Personel, göreve başlama esnasında Personel Daire Başkanlığınca Personel Bilgi Sistemine kaydedilir. Personel Bilgi Sisteminde, ilgili personelin statüsüne göre akademik/idari personel rolü/yetkisi ile Üniversite uygulama erişimi kullanıcı hesabı, kartlı geçiş sistemi hesabı ve e-posta hesabı oluşturulur.

3. Misafir personel ise Personel Daire Başkanlığınca Personel Bilgi Sistemine kaydedilir. Personel Bilgi Sisteminde, ilgili personelin statüsüne göre akademik/idari personel rolü ile uygulama erişimi kullanıcı hesabı oluşturulur.

4. Öğrenci ve misafir öğrenci, e-Devlet üzerinden ya da ilgili birimler tarafından Öğrenci İşleri Sistemine kaydedildiğinde öğrenci rolü ile uygulama erişimi kullanıcı hesabı ve kartlı geçiş sistemi hesabı oluşturulur.

5. Kullanıcılar Üniversite tarafından belirlenen en temel düzeyde yetki ile uygulamalara erişebilirler. İş süreçleri ve gereksinimleri nedeniyle gerekiyorsa personele ayrıcalıklı erişim hakkı verilebilir.

6. Üniversite uygulamalarında kullanıcı silinmez, erişim yetkisi kaldırılır.

7. Personel, öğrenci, misafir öğrenci ve misafir personel Üniversiteden ayrıldığı bilgisi ilgili birimler tarafından Personel/Öğrenci Bilgi Sistemine işlendiğinde kartlı geçiş sistemi hesabı ile uygulamalara erişim ve e-posta hesabı pasife alınır.

8. Mezun olan öğrencilerin kartlı geçiş sistemi hesabı ve e-posta hesabı pasife alınır, uygulama erişim kullanıcı hesabı pasif edilmez, mezun rolü tanımlanır.

9. Üniversite tarafından sağlanan bir hizmet için başvuru yapan kişiler ilgili sistemlerde başvuru sahibi/aday olarak kaydedilir/tanımlanır.

10. Başvuru sahiplerine/adaylara ait bilgiler ilgili birim tarafından belirlenen kurallar ve süre dâhilinde saklanır, süre sonunda silinir ve başvuru sahiplerinin/adayların bu kurallar ve süreler dâhilinde sisteme erişmesine izin verilir.

9.4 Ayrıcalıklı Erişim Hakları ve Hesapların Gözden Geçirilmesi

1. Bilgi İşlem ve alt yapısında kullanılan tüm cihazlar ve sunucular üzerinde ayrıcalıklı erişim yetkisi, yalnızca sistem, sunucu ve uygulama yöneticilerine verilir.

2. Üniversite uygulamalarında, iş süreçleri ve görev nedeniyle personel için ayrıcalıklı erişim yetkisi verilmesi gerektiğinde ilgili birimin talebine göre Uygulama Yöneticisi Birimi tarafından yetki verilir.

3. Tedarikçi sözleşmesinin sona ermesi ya da değişmesinden hemen sonra ilgili birimin talebi ile tedarikçi ve tedarikçi çalışanlarına ait hesaplar devre dışı bırakılır ve sistem erişimi iptal edilir.

4. Personel birimden ayrıldığında, uygulama erişim yetkisinin kaldırılması/düzenlenmesi ilgili birimlerin talebine göre Uygulama Yöneticisi Birimi tarafından yapılır.

5. Üniversite uygulamaları için ayrıcalıklı erişim verme, iptal etme, değişiklik ve talep yöntemleri ve uygulama şekilleri Bilgi İşlem Daire Başkanlığı ağ sayfasında yayınlanır.

6. Birimler, her uygulama için personelin yetkilerine ilişkin envanter kaydı tutar ve periyodik olarak (yılda 2 kez) kayıtları kontrol eder, birimden ayrılan ancak erişim yetkisi kaldırılmamış personel varsa yetkiler kaldırılır ve yapılan işlem kayıt altına alınır.

9.5 Uzak Erişim Yönetimi

1. İş organizasyonu kapsamında, işyeri dışından iş süreçlerini yerine getirebilmesi amacıyla Üniversite uygulamalarına (EBYS, OGRIS, PEOS vb.) kurum dışından erişim sağlanabilir. Üniversite, uygulamalara kurum dışından erişim yöntemini değiştirilebilir ve yetki kısıtlamaları yapabilir.

2. İş sürekliliği, işletilmekte olan sistem ve yazılımlara destek verilmesi gibi nedenlerle personele, tedarikçilere ve tedarikçi çalışanlarına, Üniversite ağına ve üniversite ağında yer alan sunuculara uzak erişim yetkisi verilebilir.

3. Uzak erişim:

   a) Bilgi İşlem Daire Başkanlığı tarafından izin verilen uzak erişim ve kimlik doğrulama yöntemi ile gerçekleştirilir. Bu yöntem, veri bütünlüğünün korunmasını, erişim denetimini, mahremiyeti, gizliliğin korunmasını ve sistem devamlılığını sağlamayı amaçlar.

   b) Bilgi İşlem Daire Başkanlığı teknik işler personeline uzak erişim yetkisi verilir, personel görevden ayrıldığında yetki kaldırılır.

   c) Yapılan işin gereği ihtiyaç duyulduğunda diğer birim personeli ve tedarikçi/tedarikçi çalışanları için ilgili birimin yazılı talebi ile verilir ve kaldırılır.

4. Üniversite ağına ve üniversite ağında yer alan sistem ve sunucularına uzak erişim sağlayan kullanıcılar:

   a) Yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

   b) Üniversiteye ait gizlilik dereceli ve kritik bilgiler, uzak erişim sağlanan cihazlarda bulunduramaz.

c) Erişim için kullanılacak cihazlarda gerekli güvenlik tedbirlerini alır.

5. Personel, uzak erişim için Üniversite tarafından verilen bilgisayarı kullanır. İş sürekliliği, işletilmekte olan sistem ve yazılımlara uzaktan destek verilmesi gibi acil durumlarda, kişisel cihazlarını kullanabilir. Bu durumda, kurumsal bilgi ve verinin cihaza indirilmemesi ve işlenmemesi için gerekli özen gösterilir, çalışma süresince zorunlu olarak cihaza indirilen veri şifreli olarak saklanır ve güvenli olarak silinir.

6. Tedarikçi ve tedarikçi çalışanları, kurumsal bilgi ve veriyi uzak erişim sağlanan cihazlara indiremez ve işleyemez.

7. Uzak erişim kullanıcıları, Üniversite ağına uzaktan erişim yetkisinin gerektirdiği sorumlulukları kabul ettiğini içeren Uzak Erişim Bağlantı Taahhüt Formunu imzalar.

9.5.1 Uzak Erişim için Kullanılacak Cihazlar

1. Uzak erişim kullanıcıları, uzak erişim için kullanılacak cihaz ve ortamlarda güvenlik tedbirlerini sağlamaktan sorumludur. Bu cihaz ve ortamlarda sağlanması gereken asgari tedbirler şunlardır:

a) Güvenlik duvarı kurulu ve aktif olmalıdır.

b) İşletim sistemi ve diğer uygulamalar güncel olmalıdır.

c) Ekranın parola koruması aktif olmalıdır.

ç) Fiziki güvenliği olmayan ortamlarda kullanılan cihazlar emniyete alınmalıdır.

d) Kullanılmayan ağ özellikleri pasif hale getirilmelidir.

e) Yerel disklerinde yer alan kurumsal bilgi ve verinin yedeği sadece şifreli ortamlarda ve/veya şifreli yedeklenmiş olarak saklanmalıdır.

2. Akıllı telefon ve tabletlerde işletim sistemi kısıtlamalarından kurtulmak için “jailbreak” veya “rootlama” işlemi yapılan cihazlar uzak erişim için kullanılamaz.

3. Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır.

4. Uzak erişim parolaları cihaz üzerinde kayıtlı tutulmaz.

9.5.2 Kütüphane Kaynaklarına Erişim

Üniversite dışından kütüphane kaynaklarına erişim yetkisi verilen tüm kullanıcılar, Kütüphane ve Dokümantasyon Daire Başkanlığınca sağlanan uzak erişim hizmetini kullanabilir.