Evrak Tarih ve Sayısı: 07/12/2023-447160

T.C.
NİĞDE ÖMER HALİSDEMİR ÜNİVERSİTESİ REKTÖRLÜĞÜ
Bilgi İşlem Daire Başkanlığı

Sayı : E-47437430-050.01.04-447160 07/12/2023
Konu : Bilgi ve İletişim Güvenliği Politikası

DAĞITIM YERLERİNE

Üniversitemiz Senatosunun 29.11.2023 tarihli toplantısının 2023/293 sayılı kararına istinaden, Niğde Ömer Halisdemir Üniversitesi Bilgi ve İletişim Güvenliği Politikası Ek'te gönderilmiş olup, gerekli önlemlerin alınması ve ilgililere duyurulması hususunda;

Gereğini rica ederim.

Prof. Dr. Hasan USLU
Rektör

Ek:Bilgi ve İletişim Güvenliği Politikası (26 Sayfa)

Dağıtım:
Tüm Birimlere

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Adres:Merkez Yerleşke Bor Yolu 51240 Niğde
Telefon:3882252220 Faks:3882252222
e-Posta:bidb@ohu.edu.tr Web:http://ohu.edu.tr/bilgiislemdairebaskanligi
Kep Adresi:nohu@hs01.kep.tr

Bilgi için: Baki DEMİRCİ
Unvanı: Bilgisayar İşletmeni
Tel No: 0388 225 22 19

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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,

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

4. BİLGİ GÜVENLİĞİ POLİTİKASI

Niğde Ömer Halisdemir Üniversitesi, en üst seviyede güvenlik anlayışı içerisinde bilginin korunması gerektiği bilinci ile bilgi güvenliği ile ilgili yasal düzenlemelere ve sözleşmelere uymayı, bilginin gizliliğini, bütünlüğünü ve yetkiler dâhilinde erişilebilirliğini korumayı, bilgi güvenliğine yönelik tehditlerin etkisini azaltmayı ve güvenlik seviyesini sürekli iyileştirebilmek amacıyla gerekli kaynakları tahsis etmeyi, bilgi güvenliği konusunda Üniversitenin güvenilirliğini ve itibarını korumayı, bilgi güvenliği politikalarını uygulamayı, kontrolünü sağlamayı ve olası ihlal durumlarında gerekli yaptırımlara başvurmayı, bilgi güvenliği konusunda farkındalığını arttırmak amacıyla yetkinlikleri geliştirecek eğitimleri sağlamayı taahhüt eder.

5. İNSAN KAYNAKLARI BİLGİ GÜVENLİĞİ POLİTİKASI

5.1 Göreve Başlama ve Çalışma

1. Üniversitede, göreve başlama sürecinde tüm personel için statüsüne göre Personel Daire Başkanlığı ve İdari ve Mali İşler Daire Başkanlığı tarafından yasal mevzuata göre gerekli güvenlik kontrolleri yapılır.

2. Personele göreve başlama esnasında, Niğde Ömer Halisdemir Üniversitesi Personel Gizlilik Taahhütnamesi imzalatılır. Ayrıca, Bilgi ve İletişim Varlıklarının Kabul Edilebilir Kullanımı Politikası ve Temiz Masa Temiz Ekran Politikası kişiye tebliğ edilir. Süreç, göreve başlanılan birim tarafından yürütülür.

3. Bilgi ve iletişim varlıklarına erişim izni verilecek tedarikçi ve tedarikçi çalışanları için gerekli durumlarda yapılacak güvenlik kontrolleri, ürün ya da hizmet alan birim tarafından sağlanır, bu kişilere Gizlilik Sözleşmesi/Taahhütnamesi imzalatılır ve Bilgi ve İletişim Varlıklarının Kabul Edilebilir Kullanımı Politikası tebliğ edilir.

4. Bilgi güvenliği ihlal olaylarında, personel ve tedarikçiler için ilgili yasal mevzuat ve konuya ilişkin sözleşmeler göz önünde bulundurularak disiplin/yaptırım süreci uygulanır.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

5. Personel Daire Başkanlığınca, tüm personele düzenli aralıklarla bilgi güvenliği ve siber güvenlik farkındalık eğitimi verilmesi sağlanır. Eğitim içeriği ve kapsamı Bilgi İşlem Daire Başkanlığınca belirlenir.

6. Personel için uygulanacak personel Gizlilik Sözleşmesi/Taahhütnamesi Personel Daire Başkanlığı; tedarikçi, tedarikçi çalışanları ve 3 üncü taraflar için uygulanacak Gizlilik Sözleşmesi/Taahhütnamesi ise İdari ve Mali İşler Daire Başkanlığınca hazırlanır, güncellenir ve yayınlanır.

7. Gizlilik Sözleşmelerinde/Taahhütnamelerinde, personel ve tedarikçilerin görevlerinin/ sözleşmelerinin sona ermesi ya da istihdam koşullarının değiştirilmesinden sonra dahi bilgi güvenliği ile ilgili devam eden sorumlulukları ve uymaları gereken bilgi güvenliği kuralları belirtilir.

5.2 Görev Değişikliği ve İstihdamın Sonlandırılması

1. Görev değişikliği veya işten ayrılma ile ilgili güvenlik kontrollerinin amacı, ayrılma işlemleri esnasında yapılması gereken bilgi güvenliği ile ilgili tedbirleri almaktır.

2. İşten ayrılan personel için Personel Daire Başkanlığınca hazırlanan İlişik Kesme Formu doldurulur.

3. İşten ayrılan personel için Personel Daire Başkanlığınca, Personel Bilgi Sisteminde personel kaydı arşivlenir, bu durumda sistem tarafından erişim yetkileri ve kullanıcı hesapları kapatılır ve fiziksel erişim için kullanılan kimlik kartı geri alınır.

4. Görev yeri değişen personelin eski görevi ile ilgili erişim yetkileri ve hesapları kapatılır veya erişim yetkileri yeni görev yerinin gereksinimlerine göre yeniden düzenlenir.

5. Görev yeri değişen personelin erişim yetkilerinin kaldırılmasının/değiştirilmesinin takibi ayrıldığı birim tarafından yapılır.

5.3 Personelin Bilgi Güvenliliği Sorumlulukları

1. Personel, Üniversite Bilgi ve İletişim Güvenliği Politikalarına uygun hareket eder.

2. Personel, Üniversite Bilgi ve İletişim Güvenliği Politikasının ihlali nedeniyle Üniversite ve üçüncü kişilere vereceği her türlü zarardan sorumludur.

3. Personel, Üniversite tarafından kendisine teslim edilen veya erişim yetkisini kullanarak edindiği bilgileri, sadece görevi ile ilgili işler için kullanır, ilgili mevzuata uygun olarak korur ve işler, bilmesi gereken yetkili kişiler haricinde hiç kimse ile paylaşamaz. Bu bilgilere ilişkin yazılı veya sözlü açıklama yapamaz; kendisine veya hiçbir kişi, grup, kurum ve kuruluşa çıkar sağlamak amacıyla kullanamaz.

4. Personel, bilgi paylaşabileceği kişiler konusunda şüpheye düşerse bilginin sahibi olan veya süreci yöneten birim ile irtibata geçerek veriyi kimlerle paylaşacağını teyit eder.

5. Üniversite ve hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgi ve iletişim varlıkları içerisinde saklanan veriler, donanım-yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduğu tüm işler gizlidir ve görevin gerektirdiği durumlar haricinde kullanılamaz.

6. Personel, kullandığı bilgi işleme ortamlarını ve bu ortamlarda saklanan verileri kısmen veya tamamen tahrip etmek, değiştirmek, silmek, sistemin işlemesine engel olmak veya yanlış biçimde işlemesini sağlamak gibi davranışlarda bulunamaz.

7. Personel, görev yaptığı kurum tarafından kendisine verilen ya da tanımlanan kullanıcı adını/parolayı hiç kimseyle paylaşamaz. Kişinin kendi kusuru nedeniyle parolasının ifşa olması durumunda, başkası tarafından yapılmış olsa dahi personele teslim edilen kullanıcı adı ve parolalar ile yapılan iş ve işlemlerden ilgili personel sorumludur. Kurumdan ayrılması halinde kullandığı veri, depolama

Bu belge, güvenli elektronik imza ile imzalanmıştır.

cihazlarında oluşturduğu veri, bilgi ve tüm belgeleri, cihazları ve ofis malzemelerini eksiksiz olarak birime teslim eder ve bunların hiçbir kopyasını alamaz.

8. Personel, görev yaptığı kuruma ait sunucular üzerinden kendisine tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP adresini kullanarak gerçekleştirdiği her türlü etkinlikten, Üniversite bilgi ve iletişim varlıkları kullanılarak oluşturduğu her türlü içerikten (kayıt, doküman, yazılım vb.) sorumludur.

9. Personel, yasa gereği tutulması gereken kayıtlara ilave olarak Üniversite tarafından uygun görülen diğer sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının iz kayıtlarının hukuki süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla toplanabileceğini kabul eder.

10. Bu yükümlülükler, personelin Üniversite ile ilişkisinin sona ermesi halinde de devam eder.

6. BİLGİ VE İLETİŞİM VARLIK YÖNETİMİ POLİTİKASI

6.1 Bilgi ve İletişim Güvenliği Açısından Varlık

1. Standart envanter yönetimi bakış açısıyla, maddi değeri olan tüm varlıklar yürürlükteki ilgili yasal mevzuat uyarınca kayıt altına alınır ve belirtilen usuller ile takibi yapılır.

2. Bilgi güvenliği bakış açısıyla varlıklar; elektronik ve/veya fiziksel ortamlarda yer alan, iletişim yoluyla aktarılabilen bilgiyi içeren, Üniversitenin iş süreçleri açısından değer taşıyan tüm bilgi ve bilgi işleme olanakları, bilgiyi kullanan ve taşıyan personel ile bilgiyi barındıran fiziksel mekânlar olarak tanımlanır.

3. Üniversite tarafından; BİGR ile uyumlu, varlıkların içerdiği bilgi/verinin kritikliği göz önünde bulundurularak, aynı grup altında değerlendirilmek üzere varlık grubu ana başlıkları altında varlık grupları belirlenir.

4. Varlık gruplarının belirlenmesinde Üniversitede bulunan tüm varlıklar göz önüne alınır.

6.2 Bilgi ve İletişim Varlık Envanteri

1. Üniversite tarafından belirlenen varlık grupları çerçevesinde, birimler tarafından varlık envanteri oluşturulur.

2. Envanter kaydı, varlık grubu bazında liste olarak veya sistem üzerinde tutulur.

3. Her bilgi ve iletişim varlığı envantere kaydedilir, değişiklikleri envantere yansıtılır ve güncel olması sağlanır, başka bir birime aktarılan ve kullanım ömrünü tamamlayıp imha edilen varlıklar envanterden silinir.

4. Yeni tedarik edilen donanımlar, varlık envanterine kaydı yapılmadan Üniversite ağına bağlanmaz.

5. Birim yöneticileri, varlıkları envantere doğru olarak kaydedilmesi, izlenmesi, uygun şekilde sınıflandırılması, korunması, bu varlıklara erişecek kişi veya süreçler için erişim izinlerinin planlanması ve imha edilmesinden sorumludur.

6. BİGR kapsamında varlık grupları için envanter kaydı:

   a) Ağ ve Sistemler varlık grubu ana başlığı ve Uygulamalar varlık grubu ana başlığı için BGYS kapsamında Bilgi İşlem Daire Başkanlığınca oluşturulur ve izlenir.

   b) Taşınabilir Cihaz ve Ortamlar varlık grubu ana başlığı ve Nesnelerin İnterneti Cihazları (IoT) varlık grubu ana başlığı ile Tedarikçi Çalışanı varlık grubu tüm birimler tarafından oluşturulur ve izlenir.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

c) Birim tarafından temin edilmiş bir uygulama varsa temin eden birim tarafından oluşturulur ve izlenir.

ç) Kameralar varlık grubu, birimler ve Üniversite güvenlik birimince oluşturulur ve izlenir.

d) Fiziksel Mekânlar varlık grubu ana başlığı, birimler tarafından MEKSİS'te oluşturulur ve izlenir.

e) Çalışanlar varlık grubu, Personel varlık grubu ana başlığında Personel Daire Başkanlığınca Personel Bilgi Sisteminde oluşturulur ve ilgili birimlerce izlenir.

7. Kişisel Veri ve Özel Nitelikli Kişisel Veri envanteri işlemleri, veriyi işleyen birimler tarafından sağlanır.

8. Personel ve diğer kullanıcılar, iş akitleri, sözleşmeleri veya anlaşmaları sona erdiğinde ellerinde olan tüm kurumsal varlıkları iade etmekle sorumludur.

6.3 Bilginin Sınıflandırılması ve İşlenmesi

1. Bilgi ve iletişim varlıkları, içerdikleri bilgi/veri, kurum için taşıdıkları önem ve yasal zorunluluklar dikkate alınarak uygun bir şekilde sınıflandırılır, gizlilik derecesi belirlenir. Bilgi ve iletişim varlığının sınıflandırılmasından ilgili birim yöneticisi yetkili ve sorumludur.

2. BİGR kapsamında oluşturulan Varlık Grubunun kritiklik derecesine göre rehberde belirtilen tedbirler uygulanır.

3. Bilgi sınıflandırılmasında, 26/04/2022 tarihli ve 31821 sayılı Resmi Gazete'de yayımlanan Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik sınıflandırması uygulanır. Buna göre;

a) Çok Gizli: Açıklanması veya yetkisiz kişilerce öğrenilmesi hâlinde Devletin dış ilişkilerine, millî savunmasına, millî güvenliğine ve müttefiklerle olan faaliyetlerine önemli derecede zarar verebilecek bilgileri,

b) Gizli: İzinsiz açıklanması veya yetkisiz kişilerce öğrenilmesi hâlinde Devletin menfaatlerine, güvenlik, istihbarat ve teknoloji faaliyetlerine zarar verebilecek bilgileri,

c) Hizmete Özel: İzinsiz açıklanması veya yetkisiz kişilerce öğrenilmesi hâlinde herhangi bir idari faaliyete, gerçek veya tüzel kişiye, idari soruşturmaya, adli soruşturmaya ve kovuşturmaya zarar verebilecek bilgileri,

ifade eder.

4. Yukarıda sıralanan gizlilik derecelerinden hiçbirisi ile sınıflandırılmayan ve özel bir koruma gerektirmeyen bilgiler tasnif dışı olarak nitelendirilir. Tasnif dışı bilgiler için herhangi bir erişim kısıtlaması yoktur.

5. Gizlilik derecesi yüksek ve kritik bilgi/verinin bulunduğu varlıklara, taşıdığı yüksek risk değeri nedeniyle daha sıkı güvenlik tedbirleri uygulanır.

6. Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, hazırlanması, saklanması ve dağıtılmasında Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te belirtilen kurallar uygulanır.

7. Kişisel veri ve özel nitelikli kişisel veri içeren varlık en az Hizmete Özel gizlilik derecesiyle sınıflandırılır. Kişisel veri ile özel nitelikli kişisel veri sınıflandırılması ve envanter işlemleri, 6698 sayılı Kişisel Verilerin Korunması Kanunu, Niğde Ömer Halisdemir Üniversitesi Kişisel Verilerin Korunması ve İşlenmesi Politikası ve Niğde Ömer Halisdemir Üniversitesi Kişisel Veri Saklama ve İmha Politikası kapsamında yapılır.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

8. Üniversitenin iş ve işlemleri sonucunda oluşan belgelerin düzenlenmesine, gerekli şartlar altında korunmalarının teminine, herhangi bir sebepten dolayı kaybının engellenmesine, saklanmasına gerek görülmeyen belgelerin ayıklanmasına ve imhasına ilişkin olarak Devlet Arşiv Hizmetleri Hakkında Yönetmelik hükümleri uygulanır.

9. Gerekli durumlarda, fiziki ve elektronik ortamda olan bilgi varlıkları sınıflandırma derecesini gösterecek şekilde etiketlenir.

7. FİZİKSEL VE ÇEVRESEL GÜVENLİK POLİTİKASI

7.1 Genel Hususlar ve Güvenli Alanlar

1. Bilgi ve iletişim güvenliği açısından fiziksel ve çevresel güvenlik tedbirlerinin belirlenmesi ve uygulamaya alınmasının ön koşulu olarak gizlilik dereceli veya kritik bilgi ve bilgi işleme tesislerini barındıran güvenli alanlar tespit edilir ve bu alanların güvenlik sınırları tanımlanır.

2. Sunucu odaları, güvenlik kontrol merkezleri, arşiv odaları gibi kritik bilgilerin işlendiği veya saklandığı alanlar kolayca ulaşılamayacak yerlere kurulur ve bu alanlara erişim uygun yöntemler kullanılarak sınırlandırılır.

3. Üniversitede, fiziksel güvenlik sınırlarının belirlenmesi, fiziksel erişimin yetkilendirilmesi, kontrolü ve kayıt altına alınması, kimlik kontrol mekanizması, ziyaretçilerin kabul edileceği alanlar, teslimat ve yükleme alanları, güvenlik personeli ve izleme sistemleri, bina ve çevresel güvenliğin sağlanması, kayıt ve alarm sistemlerinin kurulması, yetkisiz giriş çıkışlarda uygulanacak işlemler, sabotaj hırsızlık gibi kasıt içeren durumlar ve dış ve çevresel tehditlere karşı alınacak önlemlere ilişkin politikalar ve prosedürler güvenlikten sorumlu birim tarafından oluşturulur, duyurulur ve izlenir.

4. Afet acil durumlarında yapılması gereken faaliyetler Sivil Savunma Birimi prosedürlerine göre yapılır.

7.2 Bilgi ve iletişim Varlıklarının Fiziksel Güvenliği ve Bakımı

1. Gizlilik dereceli ve kritik bilgi/verinin bulunduğu bilgi ve iletişim varlıkları yetkisiz kişilerin erişebileceği yerlere konumlandırılmaz, özel koruma gerektiren malzemeler ise gerekli koruma seviyesi için izole edilir.

2. Bilgi ve iletişim varlıklarına yetkisiz kişilerin fiziksel erişimini engelleyecek güvenlik tedbirleri alınır, yetkisiz kişilerin fiziksel erişiminin tespiti durumunda ilgili birim yöneticisi bilgilendirilir.

3. Donanım varlıkları birim yöneticisinin bilgisi dışında başka bir yere taşınamaz veya başka bir donanımla yeri değiştirilemez.

4. Çalışma ortamlarında, gizlilik, bütünlük ve erişilebilirliği sağlamak amacıyla Temiz Masa Temiz Ekran Politikası uygulanır.

5. Bilgi ve iletişim varlıkları, olumsuz fiziksel etkilere karşı üretici tarafından tavsiye edilen saklama ve kullanım koşullarına uyumlu olarak kullanılır; ısı, kirlilik ve diğer çevresel tehlikelerden korunur; sistem ve altyapı odalarında, gerekirse çevresel kontrollerle ortam izlenir ve uygun tedbirler alınır.

6. Bilgi ve iletişim varlıkları yerinde bakıma tabi tutulmayacaksa bakıma gönderilmeden önce içindeki bilgiler kontrol edilir ve kritik bilgiler güvenceye alınır.

7. Gizlilik dereceli ve kritik bilginin/verinin bulunduğu bilgi ve iletişim varlıkları, kullanım ömrünü tamamladığında ya da elden çıkarılacağında, bilgi/veri içeren ortamlar yasal mevzuata ve üniversite politikalarına uygun olarak imha edilir.

8. Birimlerin ihtiyaç duyması halinde, bilgisayar ve taşınabilir bilgisayarların, biçimlendirilmesi, işletim sistemi ya da lisanslı uygulama kurulması için Bilgi İşlem Daire Başkanlığınca destek sağlanır. Bu işlem için ilgili birim tarafından öncelikle Bilgisayar Format ve Kurulum Talep Formu düzenlenerek

Bu belge, güvenli elektronik imza ile imzalanmıştır.

resmi yazı ile birlikte Bilgi İşlem Daire Başkanlığına gönderilir. Bu işlemin ardından bilgisayar Bilgi İşlem Daire Başkanlığına teslim edilir.

9. Bilgi ve iletişim varlıklarının erişilebilirliğinin korunması amacıyla, destekleyici altyapı hizmetleri (jeneratör, ups, klima, elektrik hatları vb.) bakımları için Yapı İşleri ve Teknik Daire Başkanlığı ve ilgili birimler tarafından periyodik bakım programı oluşturulur, bu program dâhilinde düzenli bakımları yapılır ve yapılan bakımlar kayıt altına alınır.

10. Bilgi ve iletişim varlıklarının bakımı, tedarikçinin önerdiği sıklıkta ve şekilde yapılır, yapılan bakımlar tarih ve kontrol ayrıntılarını içerecek şekilde ilgili birimler tarafından kayıt altına alınır.

7.3 Üniversite Dışına Çıkarılan Bilgi ve İletişim Varlıklarının Güvenliği

1. Bilgi ve iletişim varlıkları izinsiz ve yetkisiz olarak Üniversite dışına çıkarılamaz, zorunlu olarak dışarı çıkarılacak tüm varlıklar için ilgili birim yöneticisinden onay alınır ve bu varlıkların ilgili birimlerce kaydı tutulur.

2. Üniversite dışında bilgi ve iletişim varlığı kullanmasına izin verilen kullanıcı, bu varlıkların, ilgili mevzuatlara, politika, prosedür ve talimatlara göre kullanılması, fiziksel güvenliği, içerdiği ve erişilen bilginin/verinin güvenliğinin sağlanmasından sorumludur.

3. Üniversite dışına çıkarılmasına izin verilen gizlilik dereceli ve kritik bilginin/verinin saklandığı varlık içerisinde yer alan veri şifrelenir ve bu amaçla kullanılan cihazlar birim tarafından kayıt altına alınır.

8. BİLGİ VE İLETİŞİM VARLIKLARI İMHA POLİTİKASI

1. Bilgi ve veri içeren ortamlar (elektronik ya da elektronik olmayan) güvenli bir şekilde depolanır ve kullanım ömrünü tamamladığında veya kullanımdan kaldırılacağı zaman veri sızıntısını önlemek amacıyla güvenli bir şekilde imha edilir. İmha işlemlerinde verinin geri dönüşümü ya da yeniden kullanılabilir hale gelmesinin önüne geçilir.

2. İmha işleminde bilginin/verinin açığa çıkmaması ve başkalarının eline geçmemesi esas alınır.

3. Bilgi/veri içeren ortamlarda, tüm parçalar elden çıkarılmadan fiziksel olarak imha edilir.

4. Bilgi/veri içeren ortamlar, yeniden kullanılmadan önce herhangi bir kritik veri ve/veya lisanslı yazılım varsa kaldırılır, cihazın içerdiği bilginin bir daha okunamaması için işlem yapılır.

5. Bilgi/veri yedeklenmesinde kullanılan ve bilgi/veri içeren ortamların güvenli imhası için işletilecek yöntemler belirlenirken bilgi ve verinin kritikliği ve sınıfı göz önünde bulundurulur.

6. Devlet Arşiv Hizmetleri Hakkında Yönetmelik kapsamındaki belge ve ortamlar ilgili yönetmelik kapsamında imha edilir ve kayıt altına alınır.

7. Gizlilik dereceli belgelerin imha sürecinde Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik uygulanır.

8. Kişisel veri, özel nitelikli kişisel veri ve bu verileri içeren ortamların imhasında Niğde Ömer Halisdemir Üniversitesi Kişisel Veri Saklama ve İmha Politikası uygulanır.

9. Bilginin/verinin imhasında ve veri içeren ortamın imhasında gizlilik ve kritikliğine göre onay gereksinimi var ise imha öncesinde ve sonrasında denetim kaydı tutulur.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

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.

11. YEDEKLEME POLİTİKASI

1. Bilgi ve veri içeren varlıklarda oluşabilecek beklenmedik durumlar karşısında, en kısa sürede erişilebilirliğini sağlamak ve olası kayıpları en aza indirmek amacıyla sistem bilgisi ve kurumsal veri düzenli olarak yedeklenir.

2. Üniversitenin sistem, sunucu, network, uygulama ve veri tabanları üzerinde kayıtlı bilgilerin yedekleme işlemi Bilgi İşlem Daire Başkanlığınca sağlanır. Bu sistemler için yedekleme sıklığı ve saklama süreleri verinin kritikliğine göre belirlenir ve dokümante edilir, yedekleme işlemi için yeterli sayı ve kapasitede yedekleme ortamı temin edilir ve farklı bir lokasyonda yedekler saklanır.

3. Üniversitenin bilgi ve verisini içeren bilgisayar, taşınabilir cihaz ve taşınabilir ortamlar için herhangi bir sorunla karşılaşıldığında sorun öncesine dönüşü sağlayacak şekilde harici bir ortamda veriler yedeklenir. Yedekleme işlemi cihaz kullanıcısı personel tarafından gerçekleştirilir.

4. Yedeklemeler için yedekleme sıklığı ve yedekleme ortamları birim yöneticisi tarafından belirlenir; envanter kaydının tutulması ve yedekleme ortamlarına sadece yetkili kişilerce erişilmesi sağlanır.

12. TEMİZ MASA TEMİZ EKRAN POLİTİKASI

1. Çalışma saatleri dışında ofis kapıları kilitli tutulur.

2. Çalışma saatleri dışında bilgisayarlar kapalı ya da ekran kilitli şekilde bırakılır.

3. Bilgisayarlara parola tanımlanır, belli bir süre kullanılmadığı zaman otomatik olarak parola ile oturum açılması sağlanacak şekilde ayarlanır.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

4. Gizlilik dereceli belgeler ve gizlilik dereceli kişisel ve özel nitelikli kişisel veri içeren taşınabilir cihazlar ve ortamlar, masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulundurulmaz, personelin yanında ya da güvenli bir alanda bulundurulur.

5. Gizlilik dereceli ve kritik bilgi/veri içeren belge basılması söz konusu olduğunda yazıcıların başında durulur ve basılmış çıktıların kontrolsüz ortamda kalmasına izin verilmez.

6. Kasa, dolap ve çekmece anahtarları masa üzerinde bırakılmaz.

7. Parolalar, kağıt ve ajanda gibi matbu ortamlarda yazılı olarak bulundurulmaz.

8. Bilgisayar ekranları ve klavyeler kullanıcısı haricindeki kişilerin göremeyeceği şekilde konumlandırılır.

9. Fotokopi, faks ve yazıcı gibi cihazlarının belleğinde bulunan gizlilik dereceli ve kritik bilgiler silinir, bu cihazlar üzerinde kritik ve gizli bilgileri içeren dokümanlar bırakılmaz.

10. Gizlilik dereceli belgeler, Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik kapsamında muhafaza ve imha edilir.

11. Kişisel veri ve özel nitelikli kişisel veri içeren belgeler ve ortamlar Niğde Ömer Halisdemir Üniversitesi Kişisel Veri Saklama ve İmha Politikası kapsamında saklanır ve imha edilir.

13. İHLAL OLAYI YÖNETİMİ POLİTİKASI

13.1 Bilgi Güvenliği İhlal Olayı

1. Bilgi Güvenliği İhlal Olayı, Üniversite bilgilerinin gizliliğini, bütünlüğünü veya erişilebilirliğini etkileyen ya da etkileme potansiyeline sahip herhangi bir olaydır.

2. Bilgi güvenliği ihlal olayları, bilgi ve iletişim varlıklarının çalınması, kaybolması ya da kırılması, bu varlıkların Üniversite politika, prosedür ya da yasa ve yönetmeliklere uygunsuz kullanımı, fiziksel güvenlik düzenlemelerinin ihlali, yetkisiz fiziksel erişim, insan hatalarından kaynaklanan ihlaller, gizli bilginin ifşa edilmesi ve siber saldırılar gibi nedenlerle olabilir.

3. Bilgi güvenliği ihlal olaylarında bildirim, müdahale ve değerlendirme süreçlerindeki tüm işlemler süreç yöneticisi birim tarafından kayıt altına alınır.

4. İhlal olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.

13.2 Bilgi Güvenliği İhlal Olay Bildirimi

1. Tüm personel, tedarikçi, tedarikçi çalışanı ve diğer kullanıcılar bilgi güvenliği çerçevesinde oluşan olağan dışı durumları bildirmekle yükümlüdür.
2. İhlal olayını fark eden personel ve öğrenci, olayla ilgili olarak ivedilikle Birim/Bölüm Yöneticisini bilgilendirir.

3. Tedarikçiler ve tedarikçi çalışanları, ihlal olaylarını kendi yönetimlerine ve hizmet sağladıkları birim yöneticisine mümkün olan en kısa sürede bildirir.

4. İhlal olayları diğer kurumlardan (USOM, ulakbim, kvkk vb.), özel ve tüzel kişilerden yazılı ya da farklı iletişim kanalları kullanılarak da Üniversiteye bildirilebilir.

13.3 Bilgi Güvenliği İhlal Olayına Müdahale

1. Kullanıcılar tarafından bildirilen ihlal olayı birim yöneticisince değerlendirilir:
   a) Olay yalnızca kendi birimini ilgilendiren bir olay ise ihlali yapan kullanıcı tespit edilir, ihlalin suç unsuru içerip içermediği belirlenir ve kanıtlar toplanır.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

b) Birim yöneticisi tarafından güvenlik ihlaline neden olan kişiler için hukuki ve idari süreçler yürütülür, tüm süreç kayıt altına alınır.

c) Olay kendi birimi dışında birimleri, Üniversite genelini ya da kişileri etkiliyorsa İYS üzerinden Bilgi Güvenliği İhlal Olayı başlığı ile olay kaydı oluşturulur.

2. İYS üzerinden yapılan bildirimler Bilgi İşlem Daire Başkanlığınca değerlendirilir, Üniversite Bilgi Güvenliği Yöneticisi ve SOME bilgilendirilir.

3. Siber olaylar, Kurumsal SOME Kurulum ve Yönetim Rehberi kapsamında yönetilir.

4. İhlal olayı, Üniversitenin genelini ya da diğer kurum ve kişileri etkileyecek şekilde iş sürekliliğine zarar veren, durduran, acil müdahale gerektiren ve Üniversite imajına zarar verebilecek ihlal olayları için İhlal Olay Müdahale Ekibi kurulur.

5. İhlal Olay Müdahale Ekibi; Rektör liderliğinde, Üniversite Bilgi Güvenliği Yöneticisi, Hukuk Müşaviri, Kurumsal İletişim Koordinatörü, SOME, Bilgi İşlem Daire Başkanı, Personel Daire Başkanı ve olayın durumuna göre belirlenecek personelden oluşur.

6. İhlal olayında, 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında kişisel veri ya da özel nitelikli kişisel verinin gizlilik ve bütünlüğü etkilenmişse Niğde Ömer Halisdemir Üniversitesi Kişisel Verilerin İşlenmesi Politikası ve Niğde Ömer Halisdemir Üniversitesi Kişisel Veri Saklama ve İmha Politikası kapsamında işlem yapılır.

14. TEDARİKÇİ İLİŞKİLERİ BİLGİ GÜVENLİĞİ POLİTİKASI

1. Üniversite için temin edilen mal ve hizmetlerin sağlanmasında bilgi güvenliğinin korunması ve iş sürekliliğinin sağlanması için tedarikçi/alt yüklenici ilişkilerinin ve kurallarının belirlenmesi amaçlanır.

2. Tedarik edilen ürün ya da hizmet, Üniversite bilgi ve iletişim varlıklarına erişebilen, işletebilen, depolayabilen, iletebilen bir ürün ya da tedarikçiye özel koruma ihtiyacı olan veri/bilgi teslim edilmesini, fiziki alanlarında personel çalıştırılmasını veya bilgi ve iletişim varlıklarına (uzaktan erişimler dâhil) erişim sağlanmasını gerektiren bir hizmet ise hazırlanan teknik ya da idari şartnamelerde "Bilgi Güvenliği Gereksinimleri" başlığı altında asgari hususlar yer alır.

3. Tedarikçi sözleşmeye konu yükümlülüklerini ifa ederken, Üniversite bilgi güvenliği politikalarına uymak zorunda olduğu ve Üniversite bilgi güvenliği politikalarına kurumsal web sitesinden erişilebileceği şartnamede yer alır.

4. Tedarikçi ve tedarikçi çalışanları ile Gizlilik Sözleşmesi/Taahhütnamesi imzalanacağı ve Gizlilik Sözleşmesi/Taahhütnamesi imzalanmadan ve idareye teslim edilmeden, işe başlanamayacağı şartnamede belirtilir ve sözleşme dokümanlarının boş hali şartnameye eklenir.

5. Tedarikçinin, tedarik edilen ürün ve hizmetleri sunabilmek için tedarik süresince bir alt yüklenici kullanması durumunda, alt yüklenicilerin de bilgi güvenliği gereksinimlerine uymak zorunda olduğu ve tedarikçinin, alt yükleniciler ve çalışanlarının Gizlilik Sözleşmesi/Taahhütnamesi ile ilgili yükümlüklere uymasından birinci derecede sorumlu olduğu şartnamede yer alır.

6. Tedarikçi tarafından sağlanan ürünler ya da sunulan hizmetlerde meydana gelecek değişikliklerin (versiyon güncellemeleri, barındırma koşulu güncellemeleri vb.) idarenin onayına sunulması, idare tarafından onaylandıktan sonra değişikliklerin uygulanması ve kayıt altına alınması gerektiği şartnamede yer alır.

7. Tedarikçi ya da çalışanlar tarafından bilgi güvenliği ihlali gerçekleştiğinde ihlal durumunu yazılı olarak bildirme yükümlülüğü şartnamede yer alır.

8. Tedarikçinin fikri mülkiyet hakları ve telif hakları dâhil, yasal ve düzenleyici gereksinimlere uyması ile ilgili hususlar şartnamede yer alır.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

9. Tedarikçinin mevzuatta meydana gelebilecek değişiklikler sebebi ile bilgi güvenliği kapsamında oluşacak uygulama farklılıklarına uyum sağlaması gerekliliği şartnamede yer alır.

10. Tedarik edilecek bilgi ve iletişim teknolojileri ürünlerinin ve hizmetlerinin tedarikçi zinciri boyunca bilgi güvenliğinin tedarikçi tarafından sağlanması gerekliliği şartnamede yer alır.

11. Üçüncü taraflar ile yapılan demo ve kavram ispatı (PoC) çalışmalarında, üçüncü tarafın sorumluluklarını içeren gizlilik taahhütnamesi imzalanır.

12. Tedarik edilen ürünün istenilen güvenlik kriterleri dâhilinde teslim edilmiş olduğunun doğrulanabilmesi için kabul kriterleri şartnamede belirlenir, izleme ve doğrulama metotları tanımlanır.

13. Bilgilendirme amaçlı ve olası anormal durumlardan iş sürekliliğinin korunması için tedarikçinin iletişim yöntemini ve acil durum kapsamı planını oluşturup ilgili birimler ile paylaşması gerekliliği şartnamede yer alır.

14. Tedarikçinin sözleşme aşamasından sonra görevlendireceği çalışanının kimlik bilgilerini ve yetki kapsamını ve yetkilendirilecek çalışanın görevden ayrılması durumunda yetki iptalini ilgili birime bildirmesi gerekliliği şartnamede yer alır.

15. Tedarik edilen veya hizmet alımı ile geliştirilen uygulama/yazılımlar için:

a) Uygulamanın/yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden taahhütname alınır.

b) Uygulama/yazılım ile ilgili gerekli dokümantasyonun hazırlanması, ilgili projeye ait kaynak kodların teslim edilmesi gibi hususlar açıkça tanımlanır.

c) Uygulama/yazılım üzerinde özel nitelikli kişisel veri işlenecek ise ilave güvenlik tedbirleri ile ilgili hususlar da şartnamelere eklenir.

ç) Tedarikçilerinin destek faaliyetleri kapsamında yürüttüğü işlemler izlenir ve iz kayıtları tutulur.

16. Bilgi güvenliği şartlarının sağlandığını garanti altına almak amacıyla tedarikçi hizmetleri düzenli aralıklarla gözden geçirilir ve dokümante edilir.

17. Olası güvenlik zafiyetlerinin engellenmesi için tedarikçi ve çalışanlarına verilen fiziksel ve mantıksal erişimler periyodik olarak gözden geçirilir ve ihtiyacın bitmesi durumunda verilen yetkiler kaldırılır.

15. ÇEREZ POLİTİKASI

Çerez (cookie) Politikası ile Niğde Ömer Halisdemir Üniversitesine ait web siteleri, mobil web siteleri ve mobil uygulamalarında kullanılan çerezlere ilişkin hangi amaçlarla hangi tür çerezlerin kullanıldığı ve bu çerezlerin ilgili kişi tarafından nasıl kontrol edilebileceği anlatılmaktadır. Veri sorumlusu olarak Üniversite, gerek duyulması halinde sitede ve alt uzantılarındaki mevcut çerezleri kullanmaktan vazgeçebilir, bunların türlerini veya fonksiyonlarını değiştirebilir veya siteye ve uygulamalara yeni çerezler ekleyebilir. Bu nedenle Üniversitenin, Çerez Politikasının hükümlerini değiştirme hakkı her zaman saklıdır. Güncel Çerez Politikası üzerinde gerçekleştirilmiş olan her türlü değişiklik sitede, uygulamada veya herhangi bir kamuya açık mecrada yayınlanmakla birlikte yürürlük kazanır. Son güncelleme tarihi metin sonunda bulunur. Üniversite tarafından işlenen verilerle ilgili olarak, 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında hazırlanan Niğde Ömer Halisdemir Üniversitesi Kişisel Verilerin Korunması ve İşlenmesi Politikası, Niğde Ömer Halisdemir Üniversitesi Kişisel Verilerin İşlenmesi Hakkında Aydınlatma Metni ve diğer bilgilere Üniversite web sitesinden (https://ohu.edu.tr/kvkk/) ulaşılabilir.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

15.1 Çerez Kullanım Amacı

Çerezler web sitelerinin kullanımı sırasında kullanıcı deneyimini artırmak, kullanıcı tercihlerine en uygun kişiselleştirilmiş içerikleri sunmak, sistem performanslarını takip etmek ve benzeri amaçlar için kullanılır.

15.2 Web Sitelerimizde Kullanılan Çerez Türleri

a) Oturum Çerezleri (Session Cookies): Oturum çerezleri kullanıcıların web siteleri ziyaretleri süresince kullanılan, web tarayıcısı/oturum kapatıldıktan sonra silinen geçici çerezlerdir. Bu tür çerezlerin kullanılmasının temel amacı kullanım süresince sayfaların düzgün bir biçimde çalışmasının teminini sağlamaktır.

b) Kalıcı Çerezler (Persistent Cookies): Kalıcı çerezler web sitelerinin işlevselliğini artırmak, ziyaretçilere daha hızlı ve iyi hizmet sunmak amacıyla kullanılan çerez türleridir. Bu tür çerezler kullanıcı tercihlerini hatırlamak için kullanılır.

15.3 Web Sitelerimizde Kullanılan Çerez Kategorileri

a) Kimlik Doğrulama Çerezleri (Authentication Cookies): Ziyaretçilerin, parola kullanarak web sitesine giriş yapmaları durumunda, bu tür çerezler ile ziyaretçinin web sitesinde ziyaret ettiği her bir sayfada site kullanıcısı olduğu belirlenerek kullanıcının her sayfada şifresini yeniden girmesi önlenir.

b) Kişiselleştirme Çerezleri (Customization Cookies): Kullanıcıların tercihlerini farklı web sitesinin farklı sayfalarını ziyarette de hatırlamak için kullanılan çerezlerdir. Örneğin: kullanıcının seçmiş olduğunuz dil tercihinin hatırlanması.

c) Analitik Çerezler (Analytical Cookies) : Web sitesini ziyaret edenlerin sayıları, web sitesinde görüntülenen sayfaların tespiti ve web sitesi ziyaret saatleri gibi analitik sonuçların üretimini sağlayan çerezlerdir.

15.4 Çerezlerin Veri Sahipleri Tarafından Yönetimi ve Silinmesi

Genellikle web tarayıcıları, çerezlerin kullanımına doğrudan izin verilmiş şekilde ayarlanmıştır. Veri sahipleri web tarayıcısı ayarları üzerinden çerezleri sınırlayabilir, engelleyebilir, silebilir veya cihazına çerez gönderildiğinde uyarı alacak şekilde ayarlayabilir. Farklı web tarayıcıları için farklı yöntemler kullanılması gerekebilir. Bu konuda detaylı bilgi web tarayıcılarının "Yardım" bölümünden öğrenilebilir. Üniversitemiz web sitelerine farklı cihazlar üzerinden erişiliyorsa, her bir cihaz için web tarayıcı "çerez ayarlarının" veri sahibi tarafından tercihlerine uygun olarak düzenlenmesi gerekmektedir. Mobil uygulamalarda çerez veya SDK yönetimi için cihazın Gizlilik veya Ayarlar Bölümünde yer alan yönlendirmeler takip edilebilir.

15.5 Kullanıcı Anlaşması

Kullanıcı, Üniversite web sitelerini kullandığı sürece cihazına çerezlerin yerleştirilmesini kabul etmiş sayılır. Kullanıcı, çerezleri istemiyorsa web tarayıcısı ve mobil uygulama ayarlarını tercihlerine göre düzenleyebilir. Kullanıcı, çerezleri tercih etmemesi halinde web sitesini, mobil uygulamayı veya mobil web sitesini kullanmaya devam eder fakat web sitesinin, mobil uygulamanın veya mobil web sitesinin tüm işlevlerine erişemeyebilir.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

16. BİLGİ TRANSFERİ VE İLETİŞİM GÜVENLİĞİ POLİTİKASI

16.1 Bilgi Transferi Güvenliği

1. Bilgi transferi, bilginin ilgili kişiler ya da sistemler arasında otomatik, yarı otomatik ya da manuel yöntemlerle aktarılması işlemidir. Bilgi transferinin yanlış veya yetkisiz yapılması hukuki sonuçlar doğurabilir ve taraflar için idari veya hukuki yaptırımlara neden olabilir.

2. Bilgi transferi, Bilgi ve İletişim Varlık Yönetimi Politikası, Bilginin Sınıflandırılması ve İşlenmesi başlığına uygun olarak gerçekleştirilir. Başta gizlilik dereceli bilgiler olmak üzere kritik bilgi ve verinin aktarımı için çeşitli kısıtlamalar ve yasal yaptırımlar olduğu dikkate alınır.

3. Gizlilik dereceli bilgi ve 6698 sayılı KVK kapsamında kişisel veriler ile özel nitelikli kişisel verilerin transferi, ilgili yasal mevzuat ve Üniversite Politikalarına göre sağlanır.

4. Aktarılan bilginin korunması amacıyla üçüncü taraflarla Gizlilik Sözleşmesi/Taahhütnamesi yapılır. Üçüncü taraflara bilgi transfer edilirken herhangi bir yasal mevzuat, bilgi/veri paylaşım anlaşması veya Gizlilik Sözleşmesi/Taahhütnamesi olup olmadığı kontrol edilir.

5. Bilgi transferi yapacak kişi, risklerin değerlendirilmesinden ve aktarım için en uygun yöntemin seçilmesinden sorumludur.

6. Kamu kurumlarının (YÖK, NVİ, ASAL vb.) web servisleri ile gerçekleştirilen bilgi transferinde resmi yükümlülük olarak gönderilen ve alınan verilerde ilgili kurumun şartlarına uyum sağlanır, diğer kurum, tedarikçi ve üçüncü taraflarla web servisleri ile gerçekleştirilecek bilgi transferinde güvenli yöntemler kullanılır.

16.2 İletişim Güvenliği

1. Üniversitede yürütülen faaliyetler, çeşitli iletişim yöntemleri kullanılarak ilgili kişilere iletilir. Herhangi bir iletişim şeklinin nasıl yapılacağı hususunda yasal mevzuatta düzenleme varsa öncelikle bu düzenlemeye göre işlem yapılır.

2. Üniversite personelinin iletişim bilgilerine Üniversitenin web sayfasında yayımlanan rehberde yer verilir. Rehberde; personelin adı, soyadı, unvanı, telefon numarası ve çalıştığı birime ilişkin bilgiler yer alır. Birimler, personele ilişkin rehberde yer alan bilgilerin doğruluğundan ve güncelliğinden sorumludur.

3. Üniversite içi ve dışı iletişim; resmi yazışmalar, e-posta, telefon, Üniversite uygulamaları ya da diğer kurumların uygulamaları üzerinden gerçekleştirilir.

4. Öğrenciler, öğretim elemanı ve danışmanları ile Öğrenci Bilgi Sistemi üzerinden yazılı olarak iletişim sağlayabilir. Bu iletişim kayıtları Öğrenci Bilgi Sisteminde saklanır.

5. Öğrenci ve mezunlar ilgili akademik birimlerle, personel ise Üniversite yönetimince uygun görülen birimlerle İYS üzerinden yazılı olarak iletişim sağlayabilir. Mesaj kayıtları İYS üzerinde saklanır; mesajlara ait dosya ekleri 2 (iki) yıl sonunda silinir.

6. Duyurular e-posta, web sayfası, SMS veya Üniversite içinde yer alan duyuru cihazları/panoları üzerinden gerçekleştirilir.

7. Tüm yazışmalar, Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'e ve Yükseköğretim Kurumları Saklama Süreli Standart Dosya Planı hükümlerine uygun olarak yapılır.

8. Kamuoyunu, personeli veya öğrencileri bilgilendirme amacıyla tüm akademik ve idari birimler ve bölümler için Üniversite alan adı altında web sayfası oluşturulur. Ayrıca proje, kongre, sempozyum gibi etkinlikler ve Rektörlükçe uygun görülen konular için de web sayfası oluşturulabilir.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

9. Üniversite ana sayfası Kurumsal İletişim Koordinatörlüğü tarafından, alt sayfalar ise ilgili birimler tarafından Niğde Ömer Halisdemir Üniversitesi Web Sayfası Hazırlama ve Yayınlama Yönergesine uygun olarak yönetilir.

10. Hangi duyuruların web sayfasında yayınlanacağına ilgili birimin yöneticisi (ya da yetkilendirdiği kişi) karar verir.

11. Tüm birimlerde, iş sürekliliği ve acil durum planlaması süreçlerinde ilgili otoritelerle iletişim yöntemleri tanımlanır ve yazılı hale getirilir. Acil durumlarda erişilmesi gereken kişilerin irtibat numaraları personelin kolayca ulaşabileceği bir şekilde bulundurulur.

12. Acil durumlarla ilgili her türlü iletişim ve haberleşme için Acil Durum İletişim Listesi oluşturulur, hizmet alınan ya da hizmet sağlanan kurum/kişi (elektrik, yangın, internet, güvenlik vb.) iletişim bilgileri de Acil Durum İletişim Listesinde bulunmalıdır. Bu listeye göre acil durumlarda iletişimi kimin, nasıl, ne zaman yapacağı belirtilir.

Bu belge, güvenli elektronik imza ile imzalanmıştır.