# 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.

## 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.

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.

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