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.

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.
   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.

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.