BİLGİ GÜVENLİĞİ POLİTİKASI

BİRİNCİ BÖLÜM
Amaç, Kapsam, ve Tanımlar

1. Kısa İsim

"Arkın Yaratıcı Sanatlar ve Tasarım Üniversitesi (ARUCAD) Bilgi Güvenliği Politikası".

2. Tanımlar

Bu İlkelerde geçen;

a) Üniversite: ARUCAD Üniversitesini,
b) Mütevelli Heyeti, Senato veya ilgili Yönetim Kurulu: ARUCAD Mütevelli Heyeti, ARUCAD Senatosu veya ilgili ARUCAD Yönetim Kurulunu,
c) Rektör: ARUCAD Rektörünü,
d) Bilgi Güvenliği; Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunmasını amaçlayan idari, teknik ve hukuki tedbirlerin bütününü,
e) Bilgi Varlığı; Kurumsal faaliyetler kapsamında üretilen, işlenen, saklanan veya iletilen her türlü veriyi, belgeyi, sistemi ve altyapıyı (veri tabanları, yazılımlar, donanımlar, basılı belgeler, sunucular vb.),
f) Gizlilik; Bilgiye yalnızca yetkili kişi, sistem veya süreçlerin erişebilmesini,
g) Bütünlük; Bilginin doğruluğunun, tamlığının ve yetkisiz değişikliklere karşı korunmasını,
h) Erişilebilirlik; Yetkili kullanıcıların, ihtiyaç duydukları anda bilgiye ve bilgi sistemlerine erişebilmesini,
i) Kişisel Veri; Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
j) Erişim Yetkisi; Bir kullanıcının bilgi varlıklarına hangi düzeyde erişebileceğini belirleyen yetkilendirmeyi,
k) Olay Müdahalesi; Bilgi güvenliği olaylarının etkisini azaltmak ve tekrarını önlemek amacıyla yürütülen teknik ve idari faaliyetleri,
l) PUKÖ Döngüsü (Planla-Uygula-Kontrol Et-Önlem Al); Kurumsal faaliyetlerin planlanması, uygulanması, izlenmesi ve elde edilen sonuçlara göre iyileştirilmesini esas alan kalite yönetim modelini,

ifade eder.

3. Amaç

Bu politikanın amacı; üniversitenin sahip olduğu bilgi varlıklarının **gizlilik, bütünlük ve erişilebilirliğini** korumak, bilgi güvenliği risklerini yönetmek ve kurumsal bilgi güvenliği kültürünü oluşturmak ve sürdürmektir.

4. Kapsam

Bu politika; Akademik ve idari birimleri, çalışanları, öğrencileri, mezunları ve yetkili üçüncü tarafları, fiziksel, dijital ve elektronik ortamlardaki tüm bilgi varlıklarını kapsar.

İKİNCİ BÖLÜM
Temel İlkeler ve Bilgi Güvenliği Yönetimi

5. Temel İlkeler

Üniversitemiz bilgi güvenliğini aşağıdaki ilkeler doğrultusunda sağlar:

(a) Gizlilik: Yetkisiz kişilerin bilgiye erişimini önlemek
(b) Bütünlük: Bilginin doğruluğunu ve tutarlılığını korumak
(c) Erişilebilirlik: Yetkili kullanıcıların bilgiye ihtiyaç duyduklarında erişimini sağlamak
(d) Yasal Uyum: Ulusal ve uluslararası mevzuata (BTHK, KVKK vb.) uygun hareket etmek
(e) Risk Temelli Yaklaşım: Bilgi güvenliği risklerini belirleyerek önleyici ve iyileştirici tedbirler almak
(f) Sürekli İyileştirme: Bilgi güvenliği uygulamalarını düzenli olarak gözden geçirmek ve geliştirmek
(g) Yönetim Taahhüdü: Üst yönetim bilgi güvenliği sistemine kaynak ayırmayı ve etkin uygulanmasını taahhüt eder.

6. Kaynak Planlama ve Yönetimi

(1) Bilgi güvenliği süreçlerinin yürütülmesi için gerekli idari, teknik ve kurumsal kaynaklar belirlenir ve sürekliliği sağlanır.
(2) Bilgi güvenliği yönetim sistemi faaliyetleri için yeterli sayıda yetkin personel görevlendirilir.
(3) Bilgi sistemlerinin güvenliğini sağlamak amacıyla gerekli donanım, yazılım ve teknolojik altyapı yatırımları planlanır ve güncel tutulur.
(4) Bilgi güvenliği risklerini azaltmaya yönelik faaliyetler için gerekli mali kaynaklar kurumsal bütçe planlamalarına dâhil edilir.
(5) Personelin bilgi güvenliği konusundaki bilgi ve becerilerini geliştirmek amacıyla eğitim ve farkındalık programları için kaynak ayrılır.
(6) Bilgi güvenliği süreçlerinde kullanılan araç ve sistemlerin sürekliliği, bakım ve güncelleme gereksinimleri düzenli olarak planlanır. Bilgi güvenliği riskleri düzenli olarak analiz edilir ve izlenir.
(7) Bilgi güvenliği sorumlulukları yetki ve görev tanımlarıyla belirlenir.

7. Bilgi Güvenliği Hedefleri

(1) Bilgi sistemlerinin sürekliliğini sağlamak,
(2) Farkındalığı artırmak,
(3) Yasal ve sözleşmesel gerekliliklere uyumu garanti altına almak,
(4) Teknik güvenlik kontrollerini sürekli güncel tutmak.

8. Bilgi Varlıklarının Korunması

(1) Bilgi varlıkları sınıflandırılır ve uygun güvenlik seviyeleri belirlenir.
(2) Fiziksel ve dijital bilgi varlıklarına erişim yetkilendirme esasına göre sağlanır.
(3) Veri kaybı, yetkisiz erişim ve siber tehditlere karşı gerekli teknik ve idari önlemler alınır.

9. Kişisel Verilerin Korunması

(1) Kişisel veriler, ilgili mevzuata uygun olarak işlenir ve korunur.
(2) Veri işleme süreçlerinde gizlilik ve güvenlik esas alınır.
(3) Yetkisiz veri paylaşımı ve ihlallerine karşı önlemler uygulanır.
(4) Risk seviyeleri belirlenir ve kontrol önlemleri tanımlanır.

10. Bilgi Güvenliği Farkındalığı

(1) Akademik ve idari personel ile öğrencilerin bilgi güvenliği farkındalığını artırmaya yönelik eğitimler düzenlenir.

(2) Bilgi güvenliği ihlallerine ilişkin bildirim mekanizmaları oluşturulur.

11. Olay Yönetimi ve İhlaller

(1) Bilgi güvenliği ihlalleri kayıt altına alınır ve analiz edilir.

(2) İhlallere karşı hızlı müdahale ve düzeltici faaliyetler uygulanır.

(3) Gerekli durumlarda ilgili merciler ve paydaşlar bilgilendirilir.

(4) Tüm kullanıcılar bilgi sistemlerinin kabul edilebilir kullanım kurallarına uymakla yükümlüdür.

12. İzleme, Denetim ve Sürekli İyileştirme

(1) Bilgi güvenliği uygulamaları düzenli olarak izlenir ve denetlenir.

(2) Denetim sonuçları doğrultusunda iyileştirici önlemler alınır.

(3) Süreçler **PUKÖ döngüsü** çerçevesinde sürekli geliştirilir.

ÜÇÜNCÜ BÖLÜM
Diğer Hususlar

13. İlkelerde Bulunmayan Haller

Bu politikada hükmü bulunmayan hallerde; ARUCAD'ın ilgili diğer mevzuat hükümleri ile Mütevelli Heyeti, Senato veya ilgili Yönetim Kurulu kararları uygulanır.

14. Yürürlüğe Giriş

Bu politikalar Arkın Yaratıcı Sanatlar ve Tasarım Üniversitesi Senatosunda kabul edildiği tarihten itibaren yürürlüğe girer.

15. Yürütme Yetkisi

Bu politikaların hükümlerini Arkın Yaratıcı Sanatlar ve Tasarım Üniversitesi Rektörü yürütür.