1. AMAÇ

Bu prosedürün amacı, verinin gerektirdiği güvenlik düzeyine uygun olarak şifrelenerek saklanması, şifrelemede kullanılan anahtarların yönetimi ve verilerin güvenli iletimi için kullanılacak yöntemlerle bunların kullanım biçimlerini belirlemektir.

2. KAPSAM

Koç Üniversitesi Bilgi Teknolojileri ve sistemleri başta olmak üzere Üniversite'nin elektronik ortamlarında yer alan tüm verileri kapsamaktadır.

3. REFERANSLAR

3.1 YÖK Öğrenci Disiplin Yönetmeliği

3.2 Koç Üniversitesi İdari Personel Yönetmeliği

3.3 COBIT.2019 kapsamında "Süreç, Organizasyonel Yapılar, Bilgi Akışları ve Varlıkları, İnsanlar, Beceriler ve Etkinlikler, Politikalar ve Prosedürler, Kültür, Etik ve Davranış, Hizmetler, Altyapı ve Uygulamalar" yönetişim bileşenlerinin ilgili yönetişim ve yönetim hedefine uygulanabilecek her biri.

3.4 ISO 27000:2013 Bilgi Güvenliği yönetim standartları ailesi tamamı.

3.5 SANS-CIS kontrolleri: En yaygın ve tehlikeli saldırıları durdurmak için belirli ve uygulanabilir yollar sağlayan, siber güvenlik eylemler dizisidir.

3.6 5651: İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

3.7 6698: Kişisel Verilerin Korunması Kanunu

3.8 4857: İş Kanunu

3.9 2547: YÖK Kanunu

4. SORUMLULUKLAR

4.1 Prosedürün yayına hazırlanmasından, onaylanmasından, yayımlanıp devreye alınmasından, iyileştirme takibinin yapılmasından, şifreleme standartlarının uygulandığının kontrol edilmesinden Bilgi Teknolojileri Direktörlüğü sorumludur.

4.2 Her hizmet ve sistem için şifreleme standartları Parola Prosedürü baz alınarak belirlenmektedir. Standartların belirlenmesinden Bilgi Güvenliği Komitesi ekibi sorumludur.

4.3 Şifrelemede kullanılacak anahtarların üretilmesinden/edinilmesinden Yazılım & Altyapı Operasyonları ekibi sorumludur.

4.4 Şifrelemede kullanılacak anahtarların saklanmasından Altyapı Operasyonları ve Bilgi Güvenliği ekibi sorumludur.

5. TANIMLAR

5.1 Üniversite (KU): Koç Üniversitesi

5.2 Rektör: Koç Üniversitesi Rektörü

5.3 Prosedür: Konfigürasyon Yönetimi Prosedürü

5.4 BT: Bilgi Teknolojileri

5.5 Veri Şifreleme: Verilerin okunabilir bir biçimden şifreli bir biçime dönüştürülmesidir.

5.6 Şifreleme Anahtarı: Verileri karıştırmak ve çözmek için açıkça oluşturulan rastgele bir bit dizisidir.

5.7 Risk: Belirli bir tehdidin bir varlığın veya varlık grubunun güvenlik açıklarından yararlanma ve dolayısıyla kuruluşa zarar verme potansiyeli.

5.8 İç Departmanlar: BT dışındaki departmanları temsil eder.

5.9 Şifre: Kullanıcının, bilgisayar sistemine veya uygulamaya kullanıcı hesabı ile birlikte kendisini tanıtmasını ve işlem yaratma ve/veya sonuçlandırmasını sağlayan, sadece kendisinin bildiği ve dilediğinde değiştirebileceği alfanümerik karakterlerden oluşan tanımdır.

5.10 Tehdit: Olumsuz bir olayın potansiyel kaynağı.

5.11 Vendor: Veri barındırma, uygulama vb. konularda hizmet veren dış tedarikçileri temsil eder.

5.12 Güvenlik Açığı: Bir sistem, uygulama veya ağda istismara veya kötüye kullanıma maruz kalan bir zayıflık.

6. TEMEL PRENSİPLER

6.1 Bu prosedür ve bağlantılı diğer yönerge ve prosedürlerin ihlal edilmesi veya ihlal edilmesine sebep olunması halinde KU İdari personeli için 4857 Sayılı İş Kanunu ve Koç Üniversitesi İdari Personel

6.2 Yönetmeliği, KU Akademik personel için 2547 Sayılı YÖK Kanunu, öğrenciler için YÖK Öğrenci Disiplin Yönetmeliği işletilmektedir.

6.3 Bu prosedüre dair tüm istisnalar ancak Bilgi Güvenliği Komitesi onayı ile uygulanmaktadır.

6.4 Güncel şifreleme teknolojileri Altyapı Operasyonları ve Bilgi Güvenliği ekibince izlenir ve değerlendirilir. BT direktörü onayı ile Üniversite gereksinimleri doğrultusunda kullanılacak olan teknolojiler belirlenir.

6.5 Belirlenen şifreleme teknolojileri Üniversite ve Üniversite verilerini barındıran tüm tedarikçilerde uygulanır.

6.6 Gerekiyorsa istemci şifreleme yazılımları temin edilir.

6.7 Üniversitede kullanılacak olan şifreleme yöntemlerinin belirlenmesi ve gerekli olması durumunda yazılımların temini Altyapı Operasyonları ve Bilgi Güvenliği ekibince yapılır. Yöntemin etkinliği ve uygunluğu belirlenir. Belirlenenler dışındaki şifreleme yöntemleri ve araçları kullanılamaz.

6.8 Yetkisiz erişim risklerini bertaraf etme ve bütünlüğü koruma amacı ile veriler şifreli iletişim kanalları üzerinden gönderilir.

6.9 Çalınma ve bilgisayara fiziksel olarak yetkisiz kişilerin erişebilmesi riskine karşı taşınabilir bilgisayarların diskleri de şifrelenir.

6.10 Bilgi sistemlerine erişim için kullanılan kimlik doğrulama verilerinin tutulduğu veritabanlarının güvenliğini sağlamaya yönelik gerekli önlemler alınır. Bunun için kimlik doğrulama verilerinin veritabanlarında şifreli olarak tutulması esas alınır.

6.11 Bu veriler kimlik doğrulama amacıyla aktarılırken şifrelenir ve verilerin aktarımı sırasında gizliliğinin sağlanmasına yönelik önlemler alınır.

6.12 Gizlilik dereceli bilgiler açık iletişim ortamlarından (örneğin; e-posta, anlık mesajlaşma v.b.) gönderileceği zaman söz konusu bilgiler şifrelenmiş ek dosya olarak iletilir. Şifreyi çözecek bilgiler bir başka kanaldan (örneğin; telefon) alıcıya iletilir.

7. YÖNTEM

7.1 Kriptografik Kontroller

7.1.1 Her ürün ve sistem için kullanılması planlanan şifreleme teknolojsi, süreç sahibi ve servis sahibi tarafından kararlaştırılmaktadır.

7.1.2 Kararlaştırılan şifreleme teknolojisinin KU güvenlik gereksinimlerine uygunluğu Bilgi Güvenliği ekibi tarafından değerlendirilmektedir.

7.1.3 Kullanılan şifreleme tekniği ve anahtarında değişiklik yapma yetkisi süreç sahibi ile sınırlandırılmaktadır.

7.1.4 Kullanılan şifreleme tekniği, anahtarı ve kullanılan anahtarın geçerlilik süresi Sharepoint listesi üzerinde tutulmaktadır.

7.1.5 Kullanılan şifreleme tekniğinin güncelliğini yitirmesi, anahtarın değişmesi veya kullanılan anahtarın geçerlilik süresinin dolması durumunda şifrelenmiş verilerin eski şifreler ile decrypt edilmesi ve yeni şifre ile tekrar encrypt edilmesi gerekmektedir.

7.1.6 İz kayıtları ve denetim izleri Log Yönetimi Prosedürü standartları kapsamında saklanmaktadır.

7.2 Anahtar Yönetimi

7.2.1 Farklı kriptografik sistemler ve farklı uygulamalar için farklı anahtarlar üretilmektedir.

7.2.2 Anahtarlara erişim yetkisine sahip kullanıcılar Sharepoint listesi üzerinde tutulmaktadır.

7.2.3 Anahtarlar çalındığında veya bir kullanıcı kurumdan ayrıldığında (bu durumda anahtarların arşivlenmesi de gerekir) ilgili anahtar iptal edilmektedir. Gerekliyse

şifrelenmiş verilerin eski anahtar ile decrypt edilmesi ve yeni şifre ile tekrar encrypt edilmesi gerekmektedir.

7.3 Anahtar Saklama Kuralları

7.3.1 İstemcilerde verilerin şifrelenmesi amacıyla kullanılan anahtarların saklanması, Yazılım & Altyapı Operasyonları sorumluluğundadır. Bu anahtarlar, gizlilik dereceli bilgi olarak ele alınmakta, başka bir kişi ile paylaşılmamakta ve güvenli ortamlarda saklanmaktadır.

7.3.2 Sunucularda ve veritabanlarında bulunan verilerin şifrelemesi amacıyla kullanılan anahtarların saklanması, Yazılım & Altyapı Operasyonları sorumluluğundadır. Bu anahtarlar, gizlilik dereceli bilgi olarak ele alınmakta, başka bir kişi ile paylaşılmamakta ve güvenli ortamlarda saklanmaktadır.

7.3.3 Sistemlerde kullanılan sertifika otoritesinden alınmış kayıtlı (registered) SSL sertifikaları sadece Yazılım & Altyapı Operasyonları ekibi ve Bilgi Güvenliği ekibi kontrolünde ilgili tedarikçi yetkilisi tarafından sistemlere yüklenir/koordine edilir. Yüklenen sertifikalar için platformun izin verdiği en yüksek erişim kısıtlaması yöntemleri uygulanır.

8. EKLER ve KAYITLAR

Yoktur.

9. GÖZDEN GEÇİRME

Bu dokümanı gözden geçirme ve güncelleştirme sorumluluğu Bilgi Teknolojileri Direktörlüğü aittir. Gözden geçirme en az yılda 1 defa yapılır. Gerekli görüldüğü zaman ve durumlarda prosedürün de revize edilmesi gereklidir.

10. DEĞİŞİKLİK/ DAĞITIM/ ONAY TABLOSU

Değişen sayfa	Tarih	Değişiklik	Değişikliği yapan
Dağıtım (İlgili Bölümler)			
Tüm Koç Üniversitesi			