MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

KRİPTOGRAFİK KONTROLLERİN KULLANIMI POLİTİKASI

İçindekiler

1. Amaç

Bu doküman, BGYS Kapsam Analizi Dokümanı'nda belirtilen, kuruluşumuz birimlerinde kritik bilginin korunması için kullanılacak olan kriptografik kontrollerin belirlenmesi amacı ile oluşturulmuştur.

2. Kapsam

Bu doküman, BGYS Kapsam Analizi Dokümanı'nda belirtilen, kuruluşumuz birimlerinde kullanılan tüm kriptografik kontrolleri kapsamaktadır.

3. Sorumluluk

Rol/Unvan / Görev	Üst Yönetim	Üst Yönetim Temsilcisi	BGYS Yöneticisi	BGYS Ekip Üyeleri	Diğer Çalışanlar
Dokümanın Hazırlanması			X	X	
Dokümanın Kontrolü			X	X	
Dokümanın Onaylanması	X	X			
Dokümanın Yayınlanması			X		
Dokümanın Güncellenmesi			X		
Dokümanın Uygulanması	X	X	X	X	X
Dokümanın Uygulamadan Kaldırılması	X	X			

4. Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Anahtar	Şifreleme metodunun fonksiyonel çıktısını belirleyen parametredir.
BGYS	Bilgi Güvenliği Yönetim Sistemi
Kriptografi	Gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür.
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri

Terim	Tanım/Açıklama
Politika	Bir şirket, kurum veya kişinin görüş, felsefe, amaç ve tutumunun belirli şekilde ifadesini, bu görüş, felsefe veya amaç doğrultusunda bir hareket planını içeren doküman tipidir.

5. Kriptografik Kontrollerin Kullanımı Politikası

Kriptografik kontrollerin uygulanmasında en az aşağıdaki maddeler uygulanır:

(1) Kriptografik kontroller ilgili yasa ve yönetmeliklere uygun olarak belirlenir.
(2) Kurumun 'Gizli' seviyeli bilgi varlıkları elektronik ortamda şifrelenerek iletilir ve saklanır. Kriptografik kontroller aşağıdaki nedenlerden dolayı kullanılır:
(a) Gizlilik: Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelenerek iletilmesi ya da saklanması.
(b) Bütünlük/Güvenilirlik: Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için elektronik imzaların veya mesaj doğrulama gibi yöntemlerin kullanılması.
(c) İnkâr edilemezlik: İstenmeyen bir olayın, faaliyetin oluştuğunun veya oluşmadığının kanıtlanması gerektiği durumlarda kriptografik tekniklerin kullanılması.
(3) Veri iletimi ve veri saklanması için kullanılacak şifreleme metotlarının farklı olması gerekmektedir. Metot seçilirken aşağıdaki kriterler göz önünde bulundurulur:

(1) Kullanılabilecek en güncel metotlar tercih edilir.
(2) Seçilecek metodun güvenlik açıkları kullanımdan önce araştırılır.
(3) Şifreleme bloğu en az 256 bit olarak seçilir.
(4) Veri iletişimi esnasında kullanılacak sertifikalar güvenilir kaynaklardan temin edilir ya da kurum tarafından üretilir.
(5) Veri barındıran ve taşıyan sistemlerin kullanacağı şifreleme metotları, işletim sistemi tarafından desteklenen ya da işletim sistemine ait şifreleme yazılımlarından seçilir.
(6) Şifrelenme yönetiminin geri dönüş sağlaması için gerekli anahtarlar farklı ortamda yedeklenir.

(4) Anahtar yönetiminde göz önüne alınacak hususlar aşağıda belirtilmiştir:

(1) Güvenlik açığı tespit edilmiş anahtarlar kurum içerisinde kullanılmaz.
(2) Anahtarlar kullanımdan kaldırılmadan önce o anahtar ile şifrelenmiş veriler üzerindeki şifreleme kaldırılır ve şifresiz erişim kontrol edilir.
(3) Kullanılmayacak anahtarlar tekrar kullanılamayacak şekilde imha edilir.
(4) Kurumda kullanılacak sertifikalar en fazla 5 yıl geçerli olacak şekilde tanımlanır.
(5) Anahtar yönetimi ile ilgili faaliyetlerin izleme kayıtları saklanır.

6. İlgili Dokümanlar

6.1. İç Kaynaklı Dokümanlar

(1) KA.01 BGYS Kapsam Analizi

6.2. Dış Kaynaklı Dokümanlar

(1) TS ISO/IEC 27001:2013 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					