1. AMAÇ

Bu Prosedürün amacı, OSTİM Teknik Üniversitesi iç ağı ile internet üzerinden "Çok Gizli, Gizli ve Hassas" bilgilerin iletimi ve saklanması sırasında uygulanması gereken kriptolama kontrollerini tanımlamaktır.

2. KAPSAM

Bu prosedür Bilgi Güvenliği Yönetim Sistemi dahilindeki tüm sistemlerde ve operasyonel süreçlerde oluşan verileri kapsamaktadır.

3. TANIMLAR

Bu prosedürde geçen;

a) Bilgi Güvenliği: OSTİM Teknik Üniversitesi'nin faaliyetlerini yürütmek için gereksinim duyduğu bilgi varlıklarının ve buna ilişkin işletimin güvenliğini,

b) BGYS: Bilgi Güvenliği Yönetim Sistemini,

c) BT Birimi: Bilgi Yönetim Daire Başkanlığı'nı,

d) Hassas Bilgi: Belirli bir dönem "Çok Gizli" veya "Gizli" sınıfında olup o dönem sonunda "Tasnif Dışı" veya "Hizmete Özel" olarak seviyesi değiştirilmiş veya süresiz olarak "Çok Gizli" veya "Gizli" sınıfında kategorize edilen bilgiyi,

e) "Çok Gizli" ve "Gizli" bilgi: Bilgi Sınıflandırma düzeninde "Çok Gizli" ve "Gizli" olarak tanımlanan bilgiyi,

f) Kriptografik Anahtar: Kriptografi algoritmasının çözülmesi amacıyla oluşturulan sayı dizisini,

g) Kriptolama: Bilginin yetkisiz kişilerce okunmasının önlenmesi için standart bir kural çerçevesinde anlaşılmayacak bir hale getirilmesini,

h) Varlık: OSTİM Teknik Üniversitesi için değeri olan ve bu nedenle uygun şekilde korunması gereken bilgi varlığı unsurları ifade eder.

ifade eder.

4. KRİPTOGRAFİK KONTROLLER

- Kriptografik kontroller, e-posta gönderimi, veri tabanı üzerinden veri iletimi, ağlar arası iletişim, web sayfaları için web servislerde SSL sertifikalar kullanılmaktadır. Microsoft 365 sertifikaları kullanılmaktadır.

- Sistemlere erişim ve sistemler arası iletişimde kullanılacak kriptografik kontrollerin belirlenmesi, temini ve uygulanmasından Bilgi Yönetim Daire Başkanı sorumludur.

- OSTİM Teknik Üniversitesi'ne ait Hassas Veriler, güvenli olmayan ağlar üzerinden karşı taraflarla şifrelenerek paylaşılır. Bu kapsamda ağlar üzerinde kriptografik kontroller uygulanır.

- Bu tür verilerin e-posta veya başka bir şekilde aktarımının şifreli olmasına dikkat edilmeli, veriler mobil cihazlar dahil şifreli biçimde saklanmalıdır.

5. ANAHTAR YÖNETİMİ

- Üretilen anahtarlar, kaybolmaya, değiştirilmeye veya yok edilmeye karşı korunmaktadır. Özel ve gizli anahtarlar kontrollü olarak Bilgi Yönetim Daire Başkanı gözetiminde oluşturulmaktadır.

- SSL anahtarları ve yedekler elektronik ortamlarda muhafaza edilir.

6. ELEKTRONİK İMZALAR VE SERTİFİKALAR

- Elektronik imzalar, imza sirkülerinde yetkisi veya vekaleti bulunan personel tarafından kullanılmaktadır.

- Elektronik imzaların bitiş sürelerinin takibi e-imza sahipleri tarafından gerçekleştirilir. Süre bitimine 1 ay kala yenileme program üzerinde yenileme alanı aktif hale gelir

7.REVİZYON GEÇMİŞİ

Revizyon No	Tarih	Açıklama
01	07.11.2024	Entegre Kalite Yönetim Sisteminde kalite yönetiminde zorluklar ile karşılaşılması sebebiyle ISO 9001 Kalite Yönetim Sistemi (KYS) ve ISO 27001 Bilgi Güvenliği Yönetim Sisteminin (BGYS) ve dokümanlarının ayrılması ve ayrı ayrı takip edilmeleri kabul edilmiştir. Bu sebeple doküman kodlamalarında revizyon yapılmıştır.

Hazırlayan	Kontrol Eden	Onaylayan
İlknur ALŞAHİN Kalite Birimi	Kenan IŞIK Kalite Koordinatörü	Prof.Dr. Murat Ali YÜLEK Rektör
E-imzalıdır/paraflıdır	E-imzalıdır	E-imzalıdır