1. Giriş

ISO 27001:2022 standardı, Kurumların bilgi güvenliğini sağlamaları için bir çerçeve sunar. Veri sızıntısı önleme, bu standardın en kritik bileşenlerinden biridir. Bu prosedür, Kurumların hassas verilerini korumak için gerekli adımları ve kontrolleri belirler.

2. Amaç

Bu prosedürün amacı, yetkisiz erişim, yanlışlıkla paylaşım veya sistem arızaları gibi nedenlerle hassas verilerin Kurum dışına çıkmasını önlemektir.

3. Kapsam

Bu prosedür, tüm bilgi varlıklarını (kağıt, elektronik veya dijital) kapsar ve veri sızıntısı riskini azaltmak için gerekli tüm kontrolleri tanımlar.

4. Sorumluluklar

Bilgi Güvenliği Yöneticisi: Prosedürün uygulanmasından genel olarak sorumludur.

Veri Sahibi: Veri sızıntısı riskini değerlendirmek ve gerekli önlemleri almakla sorumludur.

IT Departmanı: Teknik kontrolleri uygulamak ve veri sızıntısı olaylarına yanıt vermekten sorumludur.

5. Uygulama

5.1.Veri Sınıflandırması

Tüm bilgi varlıklarının hassasiyet seviyesine göre sınıflandırılması.

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

Hassas verilerin belirlenmesi ve korunması için özel önlemler alınması.

5.2.Erişim Kontrolü

"En az ayrıcalık ilkesi"ne uygun olarak kullanıcıların sadece ihtiyaç duydukları verilere erişiminin sağlanması.
Güçlü kimlik doğrulama mekanizmalarının kullanılması (örneğin, çok faktörlü kimlik doğrulama).
Erişim loglarının tutulması ve düzenli olarak incelenmesi.

5.3.Veri Şifreleme

Hassas verilerin hem hareket halindeyken hem de depolama sırasında şifrelenmesi.
Güçlü şifreleme algoritmalarının kullanılması.

5.4.Veri Kaybı Önleme (DLP) Çözümleri

DLP yazılımlarının kullanılmasıyla hassas verilerin izinsiz aktarılmasının tespiti veya engellenmesi.
E-posta, USB sürücüleri, bulut depolama gibi farklı kanallar üzerinden veri sızıntısı risklerinin azaltılması.

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

5.5.Güvenlik Farkındalığı Eğitimi

Çalışanlara veri sızıntısı riskleri ve önleme yöntemleri konusunda eğitim verilmesi.
Sosyal mühendislik saldırılarına karşı farkındalık oluşturulması.

5.6.Olay Yönetimi

Veri sızıntısı olaylarının tespiti, analizi ve yanıtlanması için süreçlerin oluşturulması.
Olay sonrası inceleme ve iyileştirme faaliyetlerinin gerçekleştirilmesi.

5.7.Yedekleme ve Kurtarma

Verilerin düzenli olarak yedeklenmesi ve yedeklerin güvenli bir ortamda saklanması.
Veri sızıntısı durumunda verilerin hızlı bir şekilde kurtarılması için planların hazırlanması.

5.8.Tedarikçi Yönetimi

Üçüncü taraf hizmet sağlayıcılarının veri güvenliği uygulamalarının değerlendirilmesi.
Sözleşmelerde veri güvenliği şartlarının belirtilmesi.

6. Ölçüm ve İzleme

Veri sızıntısı olaylarının sayısı ve türü gibi göstergelerin takip edilmesi.
DLP çözümlerinin etkinliğinin değerlendirilmesi.

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

Güvenlik farkındalığı eğitimlerinin sonuçlarının ölçülmesi.

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı