1. Giriş

ISO 27001:2022 standardı, kurumların bilgi güvenliğini sağlamaları için bir çerçeve sunar. Veri maskeleme, kişisel verilerin korunması ve güvenlik risklerinin azaltılması için önemli bir tekniktir. Bu prosedür, Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde veri maskeleme işlemlerinin nasıl yapılacağını ve hangi durumlarda kullanılacağını açıklar.

2. Amaç

Bu prosedürün amacı, test, geliştirme veya eğitim amaçlı olarak kullanılan gerçek verilere erişimi kısıtlayarak veri gizliliğini korumak ve güvenlik risklerini azaltmaktır.

3. Kapsam

Bu prosedür, Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından yönetilen bilgi sistemlerinde bulunan tüm kişisel verileri ve hassas bilgileri kapsar. Veri maskeleme işlemi; veri tabanları, dosyalar ve diğer depolama ortamlarında gerçekleştirilebilir.

4. Sorumluluklar

Bilgi Güvenliği Yöneticisi: Prosedürün uygulanmasından genel olarak sorumludur.

Veri Sahibi: Maskelenecek verilerin belirlenmesinden ve doğrulanmasından sorumludur.

Bilgi İşlem Daire Başkanlığı / İlgili Teknik Birim: Veri maskeleme işlemlerini gerçekleştirir.

5. Uygulama

5.1. Veri Sınıflandırması

Maskelenecek veriler hassasiyet seviyesine göre sınıflandırılır. Kişisel veriler, özel kategorideki kişisel veriler ve diğer hassas bilgiler ayrı olarak değerlendirilir.

5.2. Maskeleme Kuralının Belirlenmesi

• Hangi verilerin maskeleneceği (örneğin ad, soyad, T.C. kimlik numarası, kredi kartı numarası)

• Hangi maskeleme yönteminin kullanılacağı (örneğin rastgele karakterlerle değiştirme, şablonlarla değiştirme)

• Maskelenmiş verilerin kalitesinin nasıl sağlanacağı (örneğin veri türüne uygunluk)

5.3. Veri Kopyası Oluşturulması

Orijinal veri setinden bir kopya oluşturulur.

Kopyalanan veri seti üzerinde maskeleme işlemi gerçekleştirilir.

5.4. Maskeleme İşlemi

Belirlenen kurallara göre veri maskeleme aracı kullanılarak veriler maskelenir. Maskeleme işlemi sırasında verilerin bütünlüğü korunur.

5.5. Maskeleme Doğrulama

Maskelenen verilerin doğruluğu ve tutarlılığı kontrol edilir. Orijinal veri seti ile maskelenmiş veri seti karşılaştırılarak farklılıklar incelenir.

5.6. Maskelenmiş Verilerin Saklanması

Maskelenmiş veriler güvenli bir ortamda saklanır. Maskelenmiş verilere erişim yetkileri kısıtlanır.

5.7. Dokümantasyon

Tüm veri maskeleme işlemleri detaylı bir şekilde belgelendirilir. Belgelerde, maskelenen verilerin türü, miktarı, tarih ve ilgili kişiler belirtilir.

6. Ölçüm ve İzleme

- Veri maskeleme süreçlerinin düzenli olarak takip edilmesi.
- Maskelenmiş verilerin kalitesinin değerlendirilmesi.
- Veri sızıntısı olaylarının takip edilmesi.