REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH

1. Amaç

Bu prosedürün amacı, hassas verilerin korunmasını sağlamak ve yetkisiz erişimlerden korumak için veri maskeleme tekniklerinin sistematik bir şekilde uygulanmasını sağlamaktır. Veri maskeleme, gerçek verilerin gizliliğini korurken, veri üzerinde işlem yapan uygulamalara ve kullanıcılarına anlamlı fakat gerçek verilerle aynı işlevi görebilen sahte veriler sunar.

2. Kapsam

Bu prosedür, organizasyon içindeki tüm hassas verileri kapsar. Hassas veriler arasında kişisel veriler, finansal bilgiler, sağlık bilgileri ve diğer gizli bilgilerin bulunduğu veri kümeleri yer alır.

3. Tanımlar

- **Veri Maskeleme:** Hassas verilerin, gerçek verilerin gizliliğini koruyarak, belirli bir işlevi yerine getirecek şekilde dönüştürülmesi veya gizlenmesi işlemi.
- **Hassas Veri:** Gizli veya kişisel bilgileri içeren veri, yasal düzenlemelere veya iç politika gerekliliklerine göre korunması gereken veridir.

4. Sorumluluklar

- **Bilgi Güvenliği Yöneticisi:** Veri maskeleme süreçlerinin uygulanmasını denetler ve maskeleme politikalarını geliştirir.
- **BT Operasyonları Ekibi:** Veri maskeleme araçlarının kurulumu ve yönetimi, maskeleme uygulamalarının entegrasyonu ve bakımından sorumludur.
- **Veri Sahipleri:** Hassas verilerin maskeleme gereksinimlerini belirler ve ilgili veri kümesi için uygun maskeleme stratejilerini onaylar.
- **İç Denetim Ekibi:** Veri maskeleme süreçlerinin etkinliğini değerlendirir ve uygunluk denetimleri yapar.

5. Veri Maskeleme Süreci

5.1 Maskeleme İhtiyaçlarının Belirlenmesi

- **Veri Sınıflandırması:** Maskeleme gerektiren hassas veriler belirlenmelidir. Bu, veri sınıflandırma politikalarına ve gizlilik gereksinimlerine dayanarak yapılır.

- **Risk Değerlendirmesi:** Hassas verilerin hangi risklere maruz kaldığı değerlendirilmelidir. Bu değerlendirme, maskeleme gereksinimlerini ve stratejilerini belirler.

5.2 Maskeleme Yöntemlerinin Seçimi

- **Maskeleme Teknikleri:** Veri maskeleme için kullanılacak teknikler seçilmelidir. Bu teknikler aşağıdaki yöntemleri içerebilir:
    - **Yerine Koyma (Substitution):** Gerçek verilerin, gerçek verilerle aynı formatta fakat anlamlı olmayan sahte verilerle değiştirilmesi.
    - **Gizleme (Hiding):** Hassas bilgilerin belirli kısımlarının gizlenmesi (örneğin, bir kredi kartı numarasının sadece son dört hanesinin gösterilmesi).
    - **Karakter Değiştirme (Character Shuffling):** Verinin karakterlerinin rastgele değiştirilmesi.
    - **Şifreleme (Encryption):** Verilerin belirli algoritmalarla şifrelenmesi ve yalnızca yetkili kişiler tarafından çözülebilmesi.

5.3 Maskeleme Uygulamasının Gerçekleştirilmesi

- **Araç ve Yazılımlar:** Maskeleme araçlarının ve yazılımlarının uygun şekilde kurulması ve yapılandırılması sağlanmalıdır.
- **Uygulama:** Seçilen maskeleme yöntemleri, veriler üzerinde uygulanmalı ve test edilmelidir. Maskeleme işlemi sırasında verinin bütünlüğü ve kullanılabilirliği korunmalıdır.

5.4 Maskeleme Sonuçlarının Test Edilmesi ve Doğrulanması

- **Test:** Maskeleme işlemi tamamlandıktan sonra, maskeleme sonuçlarının doğruluğu ve etkinliği test edilmelidir. Testler, verinin maskeleme işleminden sonra işlevselliğini ve kullanılabilirliğini doğrulamalıdır.
- **Doğrulama:** Maskeleme sonuçlarının, belirlenen güvenlik ve gizlilik standartlarına uygun olduğundan emin olunmalıdır.

5.5 Maskeleme İşlemlerinin İzlenmesi ve Raporlama

- **İzleme:** Maskeleme işlemleri düzenli olarak izlenmeli ve sürekli olarak gözden geçirilmelidir. Maskeleme süreçlerinde herhangi bir sorun veya uyumsuzluk tespit edildiğinde düzeltici eylemler uygulanmalıdır.
- **Raporlama:** Maskeleme işlemleri ile ilgili raporlar oluşturulmalı ve yetkili kişilere sunulmalıdır. Raporlar, maskeleme işlemlerinin başarısını ve herhangi bir sorun varsa çözüm süreçlerini içermelidir.

5.6 Güvenlik ve İyileştirme

- **Güvenlik:** Maskeleme süreçlerinde veri güvenliğini sağlamak için uygun önlemler alınmalıdır. Maskeleme araçları ve yöntemlerinin güvenliğini ve etkinliğini sağlamak için düzenli kontroller yapılmalıdır.
- **İyileştirme:** Maskeleme süreçleri ve teknikleri düzenli olarak gözden geçirilmeli ve iyileştirme fırsatları belirlenmelidir. Yenilikler ve teknolojik gelişmeler doğrultusunda prosedürler güncellenmelidir.

6. Dokümantasyon

- **Belgeler:** Veri maskeleme politikaları, maskeleme işlemleri, test sonuçları, raporlar ve denetim sonuçları uygun şekilde belgelenmelidir.
- **Erişim:** Dokümantasyon, yetkili personel tarafından erişilebilir olmalı ve gizli bilgiler uygun şekilde korunmalıdır.