



T.C. SAĞLIK BAKANLIĞI

YAZILIM GELİŞTİRME, VERİTABANI VE SUNUCU GÜVENLİĞİ PROSEDÜRÜ

S.B.Ü
GAZİ YAŞARGİL EĞİTİM
VE
ARAŞTIRMA HASTANESİ

Kodu	Yayınlanma Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
				1 / 2

1. AMAÇ

S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi bünyesinde geliştirilen yazılımlar ile kullanılan veri tabanı ve sunucu sistemleri ile ilgili prosedürü tanımlamaktadır.

2. KAPSAM VE SORUMLULAR

S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi bünyesinde geliştirilen Yazılımlar ile kullanılan veri tabanı, sunucu sistemleri ve bunlardan sorumlu tüm personeli kapsamaktadır.

3. UYGULAMA

3.1. Yazılım Geliştirme Güvenliği

- 3.1.1. Kurum Üst Yönetimi tarafından sadece uygun görülen yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olunur.
- 3.1.2. Uygulama yazılımlarının kurum içerisinde mi hazırlanacağı yoksa satın mı alınacağıın belirlenmesi Kurum Üst Yönetimi tarafından tanımlanır.
- 3.1.3. Yeni alınmış veya revize edilmiş bütün yazılımlar ile hazırlanan sistemler mevcut politikalar dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilir.
- 3.1.4. Eski sistemlerdeki veriler tamamen veya ihtiyaca yönelik şekilde, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılır ve/veya uygun şekilde saklanır.

3.2. Veritabanı Güvenliği

- 3.2.1. Veri tabanı sistemleri envanteri dokümanter edilir ve bu envanterden sorumlu personel tanımlanır.
- 3.2.2. Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilir.
- 3.2.3. Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulur, yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli olarak alınması kontrol altında tutulur.
- 3.2.4. Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulur.
- 3.2.5. Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilir.
- 3.2.6. Veri tabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak uygun şekilde muhafaza edilir.

Hazırlayan	Kontrol Eden	Onaylayan



T.C. SAĞLIK BAKANLIĞI

YAZILIM GELİŞTİRME, VERİTABANI VE SUNUCU GÜVENLİĞİ PROSEDÜRÜ

S.B.Ü
GAZİ YAŞARGİL EĞİTİM
VE
ARAŞTIRMA HASTANESİ

Kodu	Yayınlanma Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
				2 / 2

3.2.7. En üst düzey veri tabanı yöneticiliği sadece İstatistik ve Bilgi İşlem Birimi tarafından yetkilendirilmiş kullanıcılara verilir.

3.2.8. Bütün şifreler düzenli aralıklarla değiştirilir. Şifre belirleme konusunda "Parola Güvenliği Politikası" esas alınır.

3.3. Sunucu Güvenliği

3.3.1. Sunucu üzerinde çalışan işletim sistemleri hizmet sunucu yazılımları anti virüs vb. koruma amaçlı yazılımlar uygun şekilde ve sürede güncellenir.

3.3.2. Kurumda bulunan sunucuların yönetiminden ilgili sunucu yönetimi için yetkilendirilmiş personel sorumludur. Görevinden ayrılan personelin tüm erişim yetkileri anında iptal edilir.

3.3.3. Sunucu kurulumları, konfigürasyonları, işletim sistemi yedeklemeleri, yamaları, güncellemeleri Uzman Bilgi İşlem Personeli tarafından yapılır.

3.3.4. Sunuculara ait bilgilerin yer aldığı envanter oluşturulur. Bu envanterde sunucuların isimleri, IP adresleri, yeri, ana görevi, üzerinde çalışan uygulamalar, işletim sistemi sürümleri yer almalıdır.

3.3.5. Sunucular ile ilgili üçüncü parti firmalar ile yapılacak çalışmalarda ilgili sunucuyla yetkilendirilmiş personel eşlik eder.

4. YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla **BGYS Disiplin Prosedürü** Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

Hazırlayan	Kontrol Eden	Onaylayan