



# NECMETTİN ERBAKAN ÜNİVERSİTESİ BİLGİ İŞLEM VERİTABANI PROSEDÜRÜ

Doküman No: PR-056

Yayın Tarihi:01.08.2018

Revizyon No: 01

Revizyon Tarihi: 01.10.2021

- 1. AMAÇ – KAPSAM :** Üniversitemiz veri tabanı yönetim sistemlerinin kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlamaktır.  
Başkanlığımız sistem odası sunucularında yer alan veri tabanları kapsam dâhilindedir.
- 2. SORUMLULAR :** Bu prosedürün oluşturulmasından ve uygulanmasından Sistem, İdari Mali Hizmetler birimi sorumludur.

### 3. UYGULAMA

#### 3.1. Genel Kurallar

- 3.1.1. Veri tabanı sunucularına ancak yetkili kullanıcılar erişmelidir.
- 3.1.2. Aynı kullanıcı kodu ile aynı anda birden fazla oturum açılmasına izin verilmemelidir.
- 3.1.3. Kritik verilere her türlü erişim işlemleri (okuma, yazma, değiştirme, silme) loglanmalıdır.
- 3.1.4. Kullanıcı aktiviteleri (yapılan tüm erişimler ve okuma, yazma, değiştirme, silme işlemleri) izlenmelidir. Veri tabanı üzerinde yapılan şüpheli işler denetlenebilmelidir. Sistemin hem etkin bir şekilde yönetilmesi hem de yetkisiz erişimlerin engellenmesi ve izlenmesi anlamında gelişmiş bir kontrol mekanizması olmalıdır.
- 3.1.5. Veri tabanında tutulacak verilerin tutarlılığı tam ve kesin bir şekilde sağlanmalıdır. Bunu sağlamak için en azından, veri onay (validation), çapraz sorgulama (cross-checking) ve mükerrer kayıt önleme gibi ölçütler uygulanmalıdır.
- 3.1.6. Veri tabanı sistem logları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.
- 3.1.7. Log kayıtlarına idarenin izni olmadan kesinlikle hiçbir şekilde erişim yapılamamalıdır. Nas,storage ortamlarında tutulan log kayıtları en az 1 ay süre ile güvenli ortamlarda saklanmalıdır.
- 3.1.8. Veri tabanı işletimi ile ilgili yetkinlikler belirlenmeli, bununla ilgili eğitimler tamamlanmalı ve güncel tutulmalıdır.
- 3.1.9. Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.
- 3.1.10. Yedekleme talimatı dokümanite edilmelidir.
- 3.1.11. Veri tabanı erişim politikaları “Kimlik doğrulama ve Yetkilendirme” prosedürü çerçevesinde oluşturulmalıdır.
- 3.1.12. Hatadan arındırma, bilgileri yedekten dönme kuralları “Acil Durum Yönetimi” prosedürüne uygun olarak oluşturulmalı ve dokümanite edilmelidir.
- 3.1.13. Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
- 3.1.14. Veri tabanı sistemlerinde yama, güncelleme, bakım ve problem çözme çalışmalarında diğer birimler bilgilendirilmelidir.
- 3.1.15. Veri yedekleme medyaları kurum dışına çıkartılmamalıdır.



# NECMETTİN ERBAKAN ÜNİVERSİTESİ BİLGİ İŞLEM VERİTABANI PROSEDÜRÜ

Doküman No: PR-056

Yayın Tarihi:01.08.2018

Revizyon No: 01

Revizyon Tarihi: 01.10.2021

- 3.1.16. İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.
- 3.1.17. Veri tabanı serverda sadece ssh, rdp, ssl ve veritabanının orijinal yönetim yazılımına açık olmalı bunun dışında ftp, telnet vb. gibi açık metin (clear text) şifreli bağlantılara kapalı olmalıdır. Ancak ftp, telnet vb. clear text bağlantılar veri tabanı serverdan dışarıya yapılabilir.
- 3.1.18. Ara yüzden gelen kullanıcılar bir tabloda saklanmalı bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmalıdır.
- 3.1.19. Veritabanı sunucusuna ancak zorunlu hallerde root veya admin olarak bağlanılmalı. Root veya admin şifresi tanımlanmış kişi/kişilerde olmalıdır.
- 3.1.20. Bağlanacak kişilerin kendi adına kullanıcı adı verilecek yetkilendirme yapılacaktır.
- 3.1.21. Veritabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.
- 3.1.22. Veritabanında bulunan farklı şemaların kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
- 3.1.23. Veritabanı sunucularına internet üzerinden erişimlere kapalı olması sağlanmalıdır.
- 3.1.24. Veritabanı sunucularına kod geliştiren kullanıcı dışında hiçbir kullanıcı bağlanıp sorgu yapamamalıdır. İstekler ara yüzden sağlanmalıdır. (örnek; Kullanıcılar tablolardan select yapamamalıdır)
- 3.1.25. Veri tabanı sunucularına giden-gelen veri trafiği mümkünse şifrelenmelidir. (Ağ trafiğini dinleyen casus yazılımlar verilere ulaşamaması için)
- 3.1.26. Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için şifreleme prosedürüne bakılmalıdır.
- 3.1.27. Veri tabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak kurumun kasasında saklanmalı ve gereksiz yere açılmamalıdır.

#### 4. BGYS KAYITLARI

- VERİ TABANI YEDEKLEME TALİMATI
- ACİL DURUM KİŞİ İLETİŞİM LİSTESİ

| HAZIRLAYAN   | KONTROL EDEN   | ONAYLAYAN        |
|--|--|------------------|
| KURUMSAL KALİTE GELİŞTİRME<br>VE AKREDİTASYON<br>KOORDİNATÖRLÜĞÜ | KURUMSAL KALİTE GELİŞTİRME VE<br>AKREDİTASYON<br>KOORDİNATÖRLÜĞÜ | KURUMSAL YETKİLİ |



**NECMETTİN ERBAKAN  
ÜNİVERSİTESİ  
BİLGİ İŞLEM VERİTABANI PROSEDÜRÜ**

Doküman No: PR-056

Yayın Tarihi:01.08.2018

Revizyon No: 01

Revizyon Tarihi: 01.10.2021