1. AMAÇ

Bu prosedürün amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında kullanılan bilgi sistemleri, sunucular, veri tabanları, uygulamalar, sistem yapılandırmaları ve kritik bilgi varlıklarına ait verilerin kayıp, bozulma, silinme, yetkisiz değişiklik ve benzeri durumlara karşı korunması**,** ihtiyaç halinde geri yüklenebilmesi ve bilgi hizmetlerinin sürekliliğinin desteklenmesidir.

Bu prosedür ile yedekleme faaliyetlerinin planlı, kontrollü, güvenli ve izlenebilir şekilde yürütülmesi amaçlanmaktadır.

2. KAPSAM

Bu prosedür; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi kapsamında işletilen ve yedeklenmesi Bilgi İşlem birimlerinin sorumluluğunda bulunan;

- fiziksel ve sanal sunucuları,
- veri tabanlarını,
- uygulama ve servis verilerini,
- sistem ve uygulama yapılandırma/ayar dosyalarını,
- kritik sistem verilerini,
- iş sürekliliği açısından gerekli diğer bilgi varlıklarını kapsar.

Yedekleme kapsamı, yedekleme sıklığı ve saklama süreleri ilgili bilgi varlığının kritiklik seviyesi, risk değerlendirmesi, iş sürekliliği ihtiyaçları ve hizmet gereksinimleri dikkate alınarak belirlenir.

3. SORUMLULUKLAR

3.1. Bilgi İşlem Birimleri

- Yedekleme altyapısını işletmek,
- Yedekleme görevlerini oluşturmak ve takip etmek,
- Yedekleme sonuçlarını izlemek,
- Başarısız yedekleme işlemlerini değerlendirmek ve gerekli düzeltmeleri yapmak,
- Yedeklerin güvenli şekilde saklanmasını sağlamak,
- Gerektiğinde geri yükleme işlemlerini gerçekleştirmek,
- Geri yükleme testlerini planlamak ve sonuçlarını kayıt altına almak.

3.2. Sistem, Ağ ve Veri Tabanı Sorumluları

- Sorumluluklarındaki sistem ve verilerin yedekleme gereksinimlerini belirlemek,
- Yedekleme işlemlerinin uygunluğunu kontrol etmek,
- Sistem değişiklikleri sonrasında gerekli yedekleme kontrollerini yapmak,

- Geri yükleme ihtiyaçlarında teknik desteği sağlamak.

3.3. Birim / Süreç Sorumluları

- Kritik bilgi ve hizmetleri belirlemek,
- Yedeklenmesi gereken bilgi ve sistemlere ilişkin ihtiyaçları ilgili Bilgi İşlem birimine bildirmek,
- Geri yükleme önceliklerinin belirlenmesine katkı sağlamak.

3.4. EYS İlgili Birimleri

Yedekleme faaliyetlerinin BGYS, KVYS, İSYS ve BTHYS kapsamında belirlenen bilgi güvenliği, kişisel veri, iş sürekliliği ve bilişim hizmetleri gerekliliklerine uyumlu yürütülmesini sağlar.

4. TANIMLAR

- **Yedek:** Bilgi veya sistem verilerinin gerektiğinde geri yüklenebilmesi amacıyla oluşturulan kopyayı,
- **Geri Yükleme:** Yedeklerden yararlanılarak veri, sistem veya hizmetin önceki kullanılabilir durumuna getirilmesini,
- **Yedekleme Görevi (Job):** Belirlenen sistem veya verilerin belirlenen zaman ve kurallara göre otomatik veya kontrollü şekilde yedeklenmesini sağlayan yapılandırmayı,
- **Tam Yedek:** Belirlenen veri veya sistemin tamamının yedeklenmesini,
- **Artımlı Yedek:** Son yedekleme işleminden sonra değişen verilerin yedeklenmesini,
- **Snapshot:** Bir sistemin veya sanal makinenin belirli bir andaki durumunu gösteren anlık kopyayı,
- **RPO (Kurtarma Noktası Hedefi):** Bir kesinti veya veri kaybı sonrasında kabul edilebilir veri kaybı süresini,
- **RTO (Kurtarma Süresi Hedefi):** Bir hizmetin veya sistemin tekrar kullanılabilir hale getirilmesi için hedeflenen süreyi, ifade eder.

5. UYGULAMA

5.1. Yedekleme Planlaması

Yedekleme işlemleri; bilgi varlığının kritiklik seviyesi, riskler, iş sürekliliği gereksinimleri, RPO/RTO değerleri ve hizmet ihtiyaçları dikkate alınarak planlanır.

Her sistem için gerekli olması halinde;

- yedekleme sıklığı,
- yedekleme yöntemi,

- saklama süresi,
- yedekleme ortamı,
- geri yükleme önceliği belirlenir.

5.2. Sanal ve Fiziksel sunucuların Yedeklenmesi

Sanal ve fiziksel sunucular için belirlenen yedekleme planına uygun olarak yedekleme görevleri oluşturulur. Sanal sunucuların yedeklenmesinde kullanılan yedekleme yazılımı ve altyapısı üzerinden belirlenen sıklık ve saklama kurallarına göre yedekler oluşturulur. Sanal sunuculara ait snapshotlar, gerektiğinde kullanılmak üzere uygun depolama alanlarında tutulabilir. **Snapshot, yedekleme işleminin yerine geçmez.** Kritik sistemlerin korunmasında belirlenen yedekleme yöntemi uygulanır.

5.3. Veri Tabanlarının Yedeklenmesi

Kritik veri tabanlarının yedekleri, belirlenen yedekleme planına uygun olarak oluşturulur. Veri tabanı yedekleme işlemlerinin başarılı olup olmadığı kontrol edilir ve gerekli kayıtlar tutulur.

5.4. Sistem ve Uygulama Ayarlarının Yedeklenmesi

Sunucu, ağ cihazı, uygulama ve diğer kritik sistemlere ait gerekli yapılandırma ve ayar dosyaları belirlenen periyotlarda yedeklenir. Yedekler mümkün olduğunda tarih ve işlem bilgileri izlenebilir olacak şekilde saklanır.

5.5. Yedeklerin Saklanması

Yedekler, asıl sistemlerden bağımsız veya farklı bir depolama ortamında tutulabilecek şekilde yapılandırılır.

Yedekleme ortamlarının;

- yetkisiz erişime,
- silinmeye,
- değiştirmeye,
- fiziksel zarara,
- kötü amaçlı yazılım ve benzeri tehditlere karşı korunmasına yönelik gerekli kontroller uygulanır.

Kişisel veri veya gizli bilgi içeren yedeklere erişim yalnızca yetkili kişilerle sınırlandırılır.

5.6. Yedekleme Sonuçlarının Kontrolü

Yedekleme işlemlerinin başarı durumu düzenli olarak kontrol edilir.

Başarısız olan yedekleme işlemleri için;

- hata nedeni belirlenir,
- gerekli düzeltme yapılır,
- ihtiyaç halinde yedekleme işlemi tekrarlanır,
- önemli veya tekrarlayan hatalar kayıt altına alınır.

5.7. Geri Yükleme İşlemleri

Veri veya sistemlerin yedekten geri yüklenmesi gerektiğinde yetkili personel tarafından işlem gerçekleştirilir.

Geri yükleme işlemlerinde;

- hangi sistem/verinin geri yüklendiği,
- kullanılan yedek,
- işlem tarihi,
- işlemi gerçekleştiren kişi,
- sonuç izlenebilir olacak şekilde kayıt tutulur.

5.8. Geri Yükleme Testleri

Yedeklerin gerektiğinde kullanılabilir olduğunun doğrulanması amacıyla belirlenen periyotlarda geri yükleme testleri yapılır. Test sonuçları değerlendirilir ve tespit edilen uygunsuzluklar için gerekli düzeltici/iyileştirici faaliyetler başlatılır.

5.9. Yedeklerin Silinmesi ve Saklama Süresinin sona Ermesi

Yedekler, belirlenen saklama süreleri boyunca muhafaza edilir. Saklama süresi sona eren yedeklerin silinmesi veya imhası, yetkilendirme ve bilgi güvenliği kurallarına uygun şekilde gerçekleştirilir.

Kişisel veri içeren yedeklerin silinmesi ve imhasında KVYS kapsamında belirlenen kurallar uygulanır.

5.10. Kesinti ve Acil Durumlarda Yedeklerin Kullanılması

Bilgi sistemlerinde meydana gelen arıza, veri kaybı, siber saldırı, afet veya benzeri durumlarda yedekler, **İş Sürekliliği ve Acil Durum Yönetimi Prosedürü** kapsamında belirlenen önceliklere göre kullanılabilir. Kritik hizmetlerin yeniden devreye alınmasında belirlenen RTO ve RPO değerleri dikkate alınır.

6. İLGİLİ DOKÜMANLAR

- Bilgi Sistemleri Yedekleme Politikası
- Sunucu Yedekleşeme İşlemleri İş Akışı
- Veri Tabanı Yedekleme İşlemleri
- Sanal Sunucu Yedeklenmesi Talimatı
- Veri Tabanı Yedekleme Talimatı
- İş Sürekliliği ve Acil Durum Yönetimi Prosedürü

6.REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	22.01.2020	İlk yayın.
001	22.01.2024	Kontrol kısmı güncellenmiştir.
002	16.09.2026	SDÜ EYS kapsamına uygun olarak; kapsam, sorumluluklar, yedekleme planlaması, sunucu/veri tabanı/ayar dosyalarının yedeklenmesi, yedeklerin korunması, geri yükleme, test, kayıt ve EYS bileşenleri yeniden düzenlenmiştir.