1. AMAÇ

Bu politikanın amacı, Konya Teknik Üniversitesi (KTÜN) Bilgi Teknolojileri hizmetlerinde kesinti sürelerini ve veri kayıplarını en aza indirmek için BT sistemlerinde yer alan verilerin düzenli ve güvenli bir şekilde yedeklenmesini, felaketten kurtarma (DR) planlarını uygulamayı ve ihtiyaç halinde yedekten dönme kurallarını belirleyerek **İş Sürekliliğini** sağlamaktır.

2. KAPSAM

Bu politika; sunucular, veri tabanları, dosya sistemleri, sanallaştırma altyapısı, ağ cihazları konfigürasyonları, sistem yapılandırmaları ve kritik hizmetlere ait tüm verileri kapsamaktadır.

3. TANIMLAR

- **Yedekleme (Backup):** Orijinal verilerin kopyalanarak güvenli bir ortamda saklanmasıdır.
- **Geri Yükleme (Restore):** Yedeklenen verilerin orijinal veya alternatif ortamlara geri getirilmesi işlemidir.
- **Tam Yedekleme(Full)**: Tüm verilerin yedeğinin alınmasıdır.
- **Artımlı Yedekleme (Incremental):** Son yedeklemeden sonra değişen verilerin yedeğinin alınmasıdır.
- **Fark Yedekleme (Differential):** Son tam yedekten sonra değişen tüm verilerin yedeğinin alınmasıdır.
- **Kurtarma Hedef Süresi (RTO):**Bir kesinti veya felaket sonrasında kritik hizmetlerin kabul edilebilir bir seviyede tekrar çalışır hale gelmesi için hedeflenen maksimum süre.
- **Kurtarma Hedef Noktası (RPO):**Bir kesinti veya felaket durumunda kaybedilebilecek maksimum veri miktarıdır (zaman cinsinden).

4. YEDEKLEME SIKLIĞI VE PLANI

Bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgileri ve kuruluş verileri düzenli olarak yedeklenmelidir.

- **Planlama:** Yedekleri alınacak sistem, dosya ve veriler için ayrıntılı yedekleme planları oluşturulmalıdır.
- **Periyot:** Yedekleme periyodu saatlik, günlük, haftalık, aylık veya periyodik zaman çizelgesine göre belirlenmelidir.
- **Özelleştirme:** Her bir sistem özelinde yedeklemenin başlama zamanı, yedekleme periyodu sıklığı ve verinin saklanma süresi gibi parametreler özelleştirilmelidir.
- **Gözden Geçirme:** Yedekleme planı, yedeklenecek sistemler değişiklik gösterebileceğinden, periyodik olarak gözden geçirilmeli ve güncellenmelidir.
- **Kapsam Dışı Veri:** Yedek ünite üzerinde gereksiz yer tutmamak üzere, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dâhil edilmemelidir.

5. YEDEKLEME ORTAMLARI

Tüm yedekleme süreçlerinde, siber risklere karşı direnci artırmak için sektördeki en iyi uygulama olan **3-2-1 Yedekleme Kuralı** uygulanır:

- **3 Kopya Veri**: Verinin bir orijinali ve en az iki (2) adet yedek kopyası bulunmalıdır.
- **2 Farklı Ortam:** Veri, iki farklı depolama teknolojisi/ortamında (örneğin Disk Ünitesi ve Manyetik Kaset veya Bulut) saklanmalıdır.
- **1 Çevrimdışı/Dış Lokasyon:** Alınan yedeklerden en az bir kopya, bir felaket anında etkilenmeyecek dış lokasyonda bulundurulmalıdır. Ayrıca en az bir kopya "ağ bağlantısı olmayan ortamda (Offline Yedekleme)" (Ör: Şifreli harici diskler veya kasetler) veya Immutable (Değiştirilemez) Yedekleme formatında saklanmalıdır.

6. YETKİLENDİRME VE SORUMLULUKLAR

- **Sistem Ekibi (BT Daire Başkanlığı):** Veri merkezinde barındırılan hizmetlere ait tüm verilerin düzenli ve güvenli biçimde yedeklenmesinden sorumludur. Yedekleme işlemleri planlı, izlenebilir ve otomasyona dayalı biçimde yürütülür; yedeklerin bütünlüğü düzenli olarak kontrol edilir.
- **Akademik ve İdari Birimler:** Kendi kontrolü altında bulunan sistemler, uygulamalar, cihazlar veya yerel sunucularda tutulan verilerin yedeklenmesinden sorumludur.
- **Eskalasyon Prosedürü:** Başarısız olan yedekleme işleri, belirlenen süre içinde (örneğin 2 saat) sistem ekibine otomatik olarak bildirilmeli ve sorun çözülene kadar üst yöneticiye eskalasyon devam etmelidir.

7. YEDEKLEME GÜVENLİĞİ

- **Şifreleme:** Tüm yedekler minimum AES-256 veya eşdeğeri algoritmalarla şifrelenmelidir.
- **Bütünlük Doğrulama:** Yedeklenen verilerin bütünlüğü SHA-256 gibi yöntemlerle periyodik olarak doğrulanmalıdır.
- **Zararlı Yazılım Taraması:** Yedeklenecek veriler ve geri yüklenen içerik, virüs/malware taramasından geçirilmelidir.
- **Kayıt Tutma (Loglama):** Tüm yedekleme ve geri yükleme işlemleri kayıt altına alınmalıdır.
- **Fiziksel Güvenlik:** Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.

8. GERİ YÜKLEME TESTLERİ

8.1. Geri Yükleme Prosedürü

- **Yetki:** Geri yükleme sadece Sistem Ekibi tarafından yapılabilir.
- **Talep Yönetimi:** Yedekten geri yükleme talepleri e-posta veya EBYS üzerinden alındıktan sonra birim amiri onayıyla kayıt altına alınarak işleme alınmalıdır.

8.2. Geri Yükleme Testleri

- **Düzenli Test:** Tüm yedekleme ortamları, geri yüklemeye hazır biçimde düzenli olarak test edilmelidir.
- **Kapsamlı Test:** Kritik sistemler için yılda en az bir defa tam kapsamlı restore testi yapılmalıdır.

9. SAKLAMA VE İMHA POLİTİKASI

- **Saklama Süresi:** Yedekler, hizmet kritikliği ve varsa ilgili yasal gereklilikler doğrultusunda belirlenen süre boyunca saklanmalıdır.
- **Güvenli İmha:** İlgili saklama süreleri dolduğunda yedekler güvenli şekilde imha edilmelidir.
- **Silme İşlemi:** Silme işlemi, geri döndürülemeyecek şekilde yapılmalıdır (ör. veri silme yazılımları, fiziksel imha vb.).

10. POLİTİKA GÜNCELLEME VE İZLEME

Bu politika yılda bir kez gözden geçirilir, BT hizmetlerindeki değişikliklere göre güncellenir ve komisyon onayıyla yürürlüğe girer.

11. YAPTIRIM

Bu politikanın ihlal edilmesi durumunda KTÜN BİLGİ GÜVENLİĞİ POLİTİKASI'nda belirtilen "POLİTİKANIN İHLALİ VE YAPTIRIMLAR" başlığı altındakiler geçerlidir.

12. YÜRÜRLÜLÜK

Bu politika, BGYS Komisyonu tarafından onaylanmasını müteakip Bilgi İşlem Daire Başkanlığının web sayfasında yayımlanarak yürürlüğe girer.

13. YÜRÜTME

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.