YEDEKLEME POLİTİKASI

1. Amaç

Bu Politikanın amacı; Sakarya Üniversitesi ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında bulunan veri ve sistem varlıklarının kaybolmasını, bozulmasını veya erişilemez hâle gelmesini önlemek; felaket durumlarında hizmet sürekliliğini sağlamak üzere yedekleme ve geri yükleme faaliyetlerine ilişkin temel ilke ve esasları belirlemektir.

2. Kapsam

Bu Politika; Sakarya Üniversitesi ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamındaki Bilgi İşlem Daire Başkanlığı (BİDB), Bilgisayar Araştırma ve Uygulama Merkezi (BAUM), Uzaktan Eğitim Araştırma ve Uygulama Merkezi (UZEM) tarafından işletilen bilgi sistemlerini, sunucuları, veri tabanlarını, dosya sistemlerini, sanal ortamları, ağ altyapısını ve yedekleme çözümlerini kapsar.

3. Sorumluluklar

3.1 Üst Yönetim

- Yedekleme altyapısı, felaket kurtarma kapasitesi ve alternatif lokasyonlara ilişkin gerekli kaynakların sağlanmasından sorumludur.

3.2 Bilgi İşlem Daire Başkanlığı (BİDB), Bilgisayar Araştırma ve Uygulama Merkezi (BAUM) ve Uzaktan Eğitim Araştırma ve Uygulama Merkezi (UZEM)

- Sorumluluk alanlarındaki sistem, uygulama ve veri tabanlarının yedekleme gereksinimlerini belirler,
- Yedekleme planının uygulanmasını ve güncelliğini sağlar,
- Geri yükleme süreçlerini ilgili birimlerle koordineli şekilde yürütür.
- Yedekten geri yükleme testlerinin planlanması ve gerçekleştirilmesini sağlar.
- Sürece ilişkin kayıtların oluşturulmasını ve izlenebilirliğini temin eder.

3.3 BGYS Ekibi

- Bu politikanın ISO/IEC 27001 standardı ile uyumunu izler.
- Politikanın gözden geçirilmesi ve gerekli güncellemelerin yapılması sürecini koordine eder.

4. Politika İlkeleri

- Bu politika kapsamındaki yedekleme, geri yükleme, test ve izleme süreçlerinin uygulanması ve kayıt altına alınmasına ilişkin esaslar, **Yedekleme ve Felaket Kurtarma Prosedürü** ile güvence altına alınır.

4.1 Yedekleme Planına Uygunluk

- Yedekleme faaliyetleri, Yedekleme Planı doğrultusunda yürütülür.
- Yedekleme türleri sistemin kritiklik düzeyi ve veri değişim sıklığı dikkate alınarak belirlenir.
- Yedekleme işlemleri servis sürekliliğini aksatmayacak şekilde planlanır

4.2 RTO ve RPO Esaslı Yaklaşım

- Sistem ve hizmetlerin kritiklik düzeyi, **Bilgi Güvenliği Risk Değerlendirme Prosedürü** kapsamında hesaplanan İş Etkisi değeri esas alınarak belirlenir.
- RTO ve RPO hedefleri, iş etki değerlendirmesi sonuçları ve teknik kapasite dikkate alınarak belirlenir ve kayıt altına alınır.
- Yedekleme stratejileri, **İş Sürekliliği ve Acil Durum Planı** ile tutarlı olacak şekilde uygulanır.

4.3 Saklama Süresi ve Koruma

- Yedekleme verileri, yasal gerekliliklere uygun süreler boyunca saklanır ve süresi dolan veriler kontrollü bir şekilde imha edilir.
- Yedekleme ortamlarına erişimler, **Erişim Kontrol Prosedürü** kapsamında sınırlandırılır.
- Yedekleme kayıtları ve logları, **Log Yönetimi ve İzleme Prosedürü** hükümlerine uygun olarak tutulur.

4.4 Test ve Doğrulama

- Yedekten geri yükleme testleri planlı ve kayıtlı şekilde yürütülür.
- Kritik sistemlerin geri yüklenebilirliği periyodik olarak doğrulanır.
- Test sonuçları raporlanır ve gerekli durumlarda **Düzeltici Faaliyet Prosedürü** kapsamında işlem başlatılır.

4.5 Geri Yükleme Süreçlerinin Kontrolü

- Geri yükleme talepleri kayıt altına alınarak yürütülür.
- Uygulama düzeyindeki sistemlere ilişkin geri yükleme süreçleri BAUM ve UZEM tarafından, kurumsal yedekleme altyapısına ilişkin süreçler ise BİDB tarafından yürütülür.
- Geri yükleme sonrası oluşan kayıtlar kontrollü şekilde imha edilir ve imha bilgileri kayıt altına alınır.

4.6 Felaket Senaryoları ve Tatbikat

- Bilgi sistemlerinin sürekliliğini etkileyebilecek olağanüstü durumlarda yedekleme ve geri yükleme süreçleri, ilgili prosedürler doğrultusunda yönetilir.
- Kurumsal hizmetlerin yeniden başlatılması **İş Sürekliliği ve Acil Durum Planı** ile koordineli şekilde yürütülür.
- Tatbikat sonuçları BGYS kapsamında değerlendirilir.

4.7 Bilgi Güvenliği Olay Yönetimi

- Yedeklerin kaybı, bozulması veya yetkisiz erişimi durumunda olay, **Bilgi Güvenliği Olay Yönetimi Prosedürü** kapsamında ele alınır.
- Uygunsuzluklar ve iyileştirme gerektiren durumlar **Düzeltici Faaliyet** süreci ile yönetilir.

5. Politikanın İhlali

- Bu politikanın hükümlerine aykırı davranılması durumunda, ilgili personel hakkında **Bilgi Güvenliği Olay Yönetim Prosedürü** ve disiplin yönetmelikleri kapsamında işlem yapılır.

6. Politikanın Gözden Geçirilmesi

- Bu politika, teknolojik gelişmeler, mevzuat değişiklikleri ve Üniversitemizin ihtiyaçları doğrultusunda yılda en az bir kez gözden geçirilir ve güncellenir.