1. AMAÇ

Bu politikanın amacı; T.C. Sağlık Bakanlığı Adana İSM, Bağlı Birimleri ve Sağlık Tesisleri bünyesindeki bilgi sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için sistem ve kurumsal verilerin düzenli olarak yedeklenmesi hususunda kuralları tanımlamaktadır.

2. KAPSAM

T.C. Sağlık Bakanlığı Adana İSM, Bağlı Birimleri ve Sağlık Tesisleri dahilinde yedeğinin alınması gereken tüm veriler ve yedekleme konusunda yetkili çalışanlar da bu politika kapsamında yer almaktadır

3. UYGULAMA

3.1. Yedekleme Yönetimi

3.1.1. Verilerin yedeklenmesi iş sürekliliğinin en temel prensipleri arasında yer alır. Donanım arızaları, yazılım hataları, kullanıcıdan kaynaklanan sorunlar ya da doğal tehditler gibi nedenlerle veri kayıpları yaşanabilir. Başarılı bir yedekleme işlemi ve yedeklenen verinin ihtiyaç anında veri kaybı olmadan kurtarılabilmesi veri yedekleme sistemlerinin en temel iki bileşenidir.

3.1.2. Yedeklerin kurumun gereksinimleri dikkate alınarak hazırlanmış olması, yönetimin konuya bakış açısını yansıtan bir yedekleme politikası doğrultusunda alınıp güvenliğinin sağlanması, saklanması ve belirli sıklıkta geri dönüş testlerinin yapılması veri kaybı riskini minimum seviyeye indirecektir. Yedekleme sisteminin kurulumu; yedeklenecek veri miktarı, yedekleme sıklığı, yedeklenen verinin zaman içerisinde değişme oranı, kabul edilebilir maksimum veri kaybı gibi parametrelere bağlıdır.

3.1.3. Yedekleme politikası; olası bir felaket durumu ya da sistem hatası sonrası gerekli tüm verilerin geri getirilebilmesini sağlayacak şekilde yedekleme kuralları tanımlanmış, etkin, yönetilebilir ve izlenebilir bir yedekleme sistemi kurulması ve işletilmesine imkân verecek şekilde hazırlanmıştır.

3.1.4. Detaylı bir yedekleme analiz çalışması yapılmalı ve politikayı sağlayacak bir yedekleme planı ortaya koyulmalıdır. Yedekleme planının asgari aşağıdaki bilgileri içermesi gerekmektedir;

3.1.4.1. Yedekleme sıklığı,

3.1.4.2. Hangi saklama ortamında ne kadar süre tutulacağı,

3.1.4.3. Hangi yedekleme türü ile yedekleneceği,

3.1.4.4. Kabul edilebilir geri dönüş süresi,

3.1.4.5. Kabul edilebilir veri kaybı süresi.

3.2. Veri Analiz Çalışması

3.2.1. Yedekleme sistemi oluşturulmasının ilk adımı detaylı bir veri analiz çalışmasıdır.

3.2.2. Analiz çalışmalarında öncelikle kuruma ait veriler kategorize edilir.

3.2.3. Kategoriler; sanal sunucular, fiziksel sunucular, veritabanları, dosyalar, PACS görüntüleri, güvenlik duvarı, saldırı tespit sistemi (IPS) gibi tüm ağ ve güvenlik cihazlarının iz kayıtları, sistem erişimlerine ilişkin iz kayıtları vb. şekilde düzenlenebilir.

3.2.4. Kategorize edilen verilerin önem dereceleri bilgi güvenliği alt komisyonu tarafından belirlenir.

3.2.5. Kritik verilerin varlık envanteri özel önem gösterilmesi gereken bir husustur. Bunun için kritik varlık listesi oluşturulmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.

3.2.6. Oluşturulan varlık envanterinde hangi sistemlerde ne tür uygulamaların çalıştığı, yedeği alınacak dizin ve dosyalar, yetkili personel ve yetki seviyeleri yer almalıdır.

3.3. Yedekleme Listelerinin Oluşturulması

3.3.1. Yedekleme sistemlerinin ve networkün gereksiz yere meşgul edilmemesi, kapasitenin verimsiz kullanılmaması, kapasite artış gereksinimlerinin öngörülebilmesi ve yedekleme yazılımı lisansının tüketilmemesi adına yedekleme listesi oluşturulur. Yedekleri alınacak sistem, dosya ve verilerin belirlenip yedekleme listesinin oluşturulmasında analiz çalışmalarından faydalanılır.

3.3.2. Kurumun sistem gereklilikleri göz önüne alınarak; Sunucular, Sanal Sunucular, Veri Tabanları, Aktif Dizin/ Etki Alanı Denetleyicisi, Güvenlik ve Ağ Cihazları gibi veri içeren platformların yedeklenmesi planlanmalıdır.

3.3.3. Yedeklenecek veriler bilgi işleme süreci içerisinde değişiklik gösterebileceğinden yedekleme listesi en az yılda 2 (iki) kez gözden geçirilmeli ve güncellenmelidir.

3.3.4. Yedekleme listeleri kapasite yönetimi planlanması için referans oluşturur.

3.4. Yedekleme Planlarının Oluşturulması

3.4.1. Başarılı bir yedekleme sistemi için kategorize edilmiş ve önceliklendirilmiş verilerin yedekleme planları oluşturulur.

3.4.2. Yedekleme planları asgari olarak; yedeklenecek bileşenin adı (host name), ulaşım yolu (ip adresi), yedekleme tipi ve sıklığı, yedek geri dönüş testi raporları gibi bilgileri içerir.

3.4.3. Kurumun gereklilikleri doğrultusunda hazırlanmış olan Yedekleme Planına göre yedeklerin düzenli aralıklarla alınması ve sürekli olarak gözden geçirilmesi gerekir.

3.5. Yedekleme Çalışmaları

3.5.1. Kritik veriler yedeklenirken iki farklı şekilde yedeklenmek üzere bir yedekleme sistemi oluşturulmalıdır. Bunlardan ilki; canlı çalışma ortamında eş zamanlı olarak kümelenmiş disk sisteminin farklı disk bölümlerine; ikincisi ise, çevrimdışı olarak varsa yedekleme sunucusu yoksa şifrelenmiş olarak harici depolama ortamlarında yedeklenmesidir.

3.5.2. Kritik olmayan veriler yedeklenirken, verilerin bir kopyası mevcut sunucular üzerinde, diğer bir kopyası çevrimdışı olarak yedekleme sunucusu veya harici depolama ortamlarında tutulur.

3.5.3. Yedekleme politikası ve planları doğrultusunda yapılan yedekleme işlemleri düzenli olarak kontrol edilmeli ve Yedekleme Kontrol Listesi ile kayıt altına alınmalıdır.

3.5.4. Kurumun yedekleme işlemlerinin başarısının ölçülmesi ve rapor oluşturulması amacıyla yedekleme başarısızlıkları izlenmeli ve kayıt altına alınmalıdır.

3.5.5. Özel nitelikli kişisel veri kategorisinde bulunan sağlık kayıtlarının yer aldığı yedekleme ortamları kriptoloji usullerine göre şifrelenir.

3.5.6. Yedekleme medyalarının acil durumlarda kullanılması gerekebileceğinden güvenilir ürünlerden seçilmeli ve düzenli periyotlarda test edilmelidir.

3.5.7. Yedekleme medyalarının bulundurulduğu ortamların fiziksel uygunluğu ve güvenliği sağlanmalı ve herhangi bir felaket anında etkilenmeyecek şekilde bilgi işlem odalarından farklı odalarda veya binalarda saklanmalıdır.

3.6. Geri Dönüş Testleri

3.6.1. Yedeklenen verilerin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için belirli aralıklarla geri dönüş testlerinin yapılması gerekir.

3.6.2. Yılda en az 2 (iki) kez geri dönüş testi yapılarak tutanakla kayıt altına alınır. Tutanakta; sunucu adı, test tarihi, önceki test tarihi, yedek türü ve yedek durumu, geri yükleme testlerinin kimler tarafından ne zaman yapıldığı, başarılı olup olmadığı gibi asgari bilgiler yer almalıdır.

3.6.3. Yedekten geri yükleme testlerinin, başarısız olması nedeniyle veri kaybı olabileceği durumu göz önüne alınarak, canlı ortamda değil gerçek ortamın aynısı olan test ortamında yapılması gerekmektedir.

3.7. Yedekleme Süreci Görev ve Sorumlulukları

3.7.1. Yedekleme politikasının işletilmesi ve zaman içerisinde günün ihtiyaçlarına göre güncellenmesi veri kaybı durumunda kurumun göreceği zararı en aza indirecektir.

3.7.2. Bu nedenle, yedekleme sistemlerinin yönetiminden, yedekleme politikasının ve yedekleme planının hazırlanmasından, uygulanmasından ve güncellenmesinden sorumlu personelin görevlendirilmesi gerekmektedir.

3.7.3. Yedekleme işleminin gerekli eğitimi almış personel tarafından yapılması sağlanmalıdır.

4. YAPTIRIM

Bilgi Güvenliği Politikalarının ve Prosedürlerinin ihlali durumunda, **Bilgi Güvenliği Disiplin Prosedürü** dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.