KURUM YEDEKLEME POLİTİKASI

1. AMAÇ: Bu politikanın amacı, Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumları kapsamındaki bilgi sistemlerinde bulunan verilerin, ihtiyaç anında veri kaybı olmadan kurtarılabilmesi için veri yedekleme planı oluşturulmasıdır.

2. KAPSAM: Bu politika, Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumları bünyesindekibilgi sistemlerini kapsamaktadır.

3. PROSEDÜR METNİ

3.1. Sağlık Müdürlüğü bağlı birim ve bağlı kurumların bilgi sistemleri yedekleme sorumlusu / personel resmi yazı ile belirlenir. Yedekleme işlemi görevleri personel tarafından yürütülerek yapılan işlemler tutanak altında kayıt edilir.

3.2. Sağlık Müdürlüğüne bağlı birim ve Kurumların kendi bünyesinde bulunan bilgi sistemleri ile ilgili Yedekleme Planı oluşturulur.

3.3. ***Bİ.PL.01 Yedekleme Planında*** hangi sistemlerin yedekleneceği, yedeklenecek verinin niteliği (kişisel veri, kurumsal veri, gizli bilgi vb.), ne tür yedek alınacağı(tam yedek, fark yedek, artırımlı yedek, transactional/log yedek gibi), yedek alma periyodları, yedekleme süresi ve yedekleme sistemi belirlenir).

3.4. ***Bİ.PL.01 Yedekleme Planı*** oluştururken verinin saklanma ve korunma gerekliliği ile kurumun sözleşme ve yasalardan doğan yükümlülükleri dikkate alınır.

3.5. Yedekleme iki türlü yapılır. Birincisi eş zamanlı olarak kümelenmiş disk sisteminin farklı disk bölümlerine ikincisi çevrimdışı olarak varsa yedekleme sunucusu yoksa şifrelenmiş harici depolama ortamlarında yedekleme yapılabilir.

3.6. "Kişisel Verileri Koruma Kanunu'nun 2018/10 sayılı kararı" uyarınca özel nitelikli kişisel verilerin barındırıldığı ortamlarda; verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi, kriptografik anahtarların farklı ortamlarda tutulması, veriler üzerinde tüm hareketlerin iz kayıtların başka ortamda güvenli olarak saklanması gerekmektedir. Veri yedekleme sırasında verinin özel nitelikli kişisel veri olması halinde, yedekleme ortamlarının yukarda belirtilen koşulları taşımasının gözetilmesi gerekir.

3.7. Yedekleme sunucusu ve ya harici depolama ortamlarına yapılan çevrimdışı yedeklemeler yedekleme sorumlusu tarafından mutlaka tutanak altına alınır.

3.8. Yedekleme planları doğrultusunda yapılan yedekleme işlemleri düzenli olarak kontrol edilerek ***Bİ.LS.01 Yedekleme Kontrol Listesi*** ile kayıt altına alınarak arşivlenir.

3.9. Yedeklenen verinin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için belirli aralıklarla geri dönüş testinin yapılması gerekir.

3.10. Geri dönüş testi; 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 bilgilerin yer aldığı tutanakla kayıt altına alınır.

3.11. Yedekten geri yükleme testleri, başarısızlık durumları göz önünde alınarak, gerçek değil, gerçek ortamın aynısı olan test ortamında gerçekleştirilir.

4. YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla BGYS Disiplin Prosedürü Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

5. İLGİLİ DOKÜMANLAR:

- ***Bİ.PL.01 Yedekleme Planı***
- ***Bİ.LS.01 Yedekleme Kontrol Listesi***