1. **AMAÇ:** Sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerine ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi için standartları belirlemek amacıyla hazırlanmıştır.
2. **KAPSAM:** Bu prosedür, Hastane bünyesindeki bilgi ve bilgi sistemlerini tamamını kapsar.
3. **KISALTMALAR:**
4. **TANIMLAR:**

**Transactional:** İşlemsel

**Kripto:** Gizli ve görünmez.

1. **SORUMLULUKLAR:** Bu prosedürün uygulanmasından ilgili kurum yöneticileri sorumludur.
2. **FAALİYET AKIŞI:**
* Kurumun bütün verisinin ve uygulamaların tamamının yedeği uygun ve düzenli olarak alınmalıdır.
* Yedekleme işlemlerinin sağlanması için yedekleme politikasına uygun olarak bir yedekleme planı oluşturulmalıdır.
* Yedekleme işlerine ait kayıtlar BYS YEDEKLEME KONTROL LİSTESİ ile kayıt altına alınmaktadır.
* Başarısız olan yedekleme işleri takip edilmeli ve yedeği alınamamış verinin yedeği alınmalıdır.
* Yedekleme medyaları etiketlenmeli ve hangi medyada hangi yedeğin bulunduğuna dair kayıtlar tutulmalıdır.
* Yedekleme medyalarının kopyaları alınarak ana sistem odasına zarar verebilecek felaketlerden etkilenmeyecek kadar uzakta ve güvenli olarak depolanmaktadır.
* Yedeklenmiş verinin düzenli aralıklarla geri döndürme testi (yılda en az 2 defa) yapılmaktadır.
* Yedekleme altyapısı, yedekleme ve geri döndürme işlemleri için talimatlar hazırlanmalıdır.
* Yedeklerin bir kopyası doğal afetlerden ve olası tehlikelerden korumak maksadıyla ana merkezden uzak bir merkezde saklanmalıdır.
* 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).
* Yedekleme Planı oluştururken verinin saklanma ve korunma gerekliliği ile kurumun sözleşme ve yasalardan doğan yükümlülükleri dikkate alınır.
* Yedekleme planları doğrultusunda yapılan yedekleme işlemleri düzenli olarak kontrol edilerek Yedekleme Kontrol Listesi ile kayıt altına alınarak arşivlenir.
* Yedekleme bilgisine uygun seviyede fiziksel ve çevresel koruma sağlanmalıdır.
* Gizliliğin önemli olduğu durumlarda yedeklemelerin kriptolu olarak alınması göz önünde bulundurulmalıdır. Bu kapsamda özellikle kişisel sağlık bilgilerinin kriptolu olarak yedeklenmesine dikkat edilmelidir.

**Veri Depolamada Dikkat Edilecek Hususlar**

* Veri yedeklemede tüm sistem yedeğinin alınıp alınmadığı “***BYS YEDEKLEME KONTROL LİSTESİ”***  kontrol edilir ve tüm sistemin yedeğinin alındığından emin olunur.
* Yedekler SBYS’ nin çalıştığı ortamın haricindeki bir ortama (Harici bellek, Yedek sunucu) alınmaktadır.
* Yedekler offline ortamda süresiz olarak saklanmaktadır.

**Veri Kurtarma:**

* Yedeklemeden geri dönüşüm sağlanıp sağlanmadığı ve veri kaybının olup olmadığı kontrol edilmelidir.
* Test “***HBYS DÖNEMLİK VERİ KURTARMA TESTİ KONTROL FORMU”*** ile kayıt altına alınmaktadır.
* Herhangi bir aksaklık durumunda iyileştirme çalışmaları (hata kodları kontrol edilip hatalar düzeltilir) başlatılmalıdır.
* Tam bir veri bütünlüğü sağlanana kadar iyileştirme çalışmalarına devam edilmektedir.