T.C. Sağlık Bakanlığı	GİRESUN İL SAĞLIK MÜDÜRLÜĞÜ YEDEKLEME POLİTİKASI			T.C. Sağlık Bakanlığı Giresun İl Sağlık Müdürlüğü
Kodu	**Yayınlama tarihi**	**Revizyon Tarihi**	**Revizyon No**	**Sayfa**
BG.PO.01	**29.08.2018**			**1/4**

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.

Yedeklerin kurumun gereksinimleri dikkate alınarak hazırlanmış, 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.

1.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 hazırlanmalıdır.

Yedekleme politikasında aşağıdaki tabloda yer alan başlıkların tanımlanmış olması gerekir.

S.Nu.	Yedeklenen Sistem	Tam Yedek	Fark Yedek	Artırımlı Yedek	Transactional /Log Yedek	Saklama Süresi
1	Veri Tabanları					
2	Sanallaştırma Sunucuları					
3	Dosya Paylaşım Platformu					
4	Aktif Dizin					

2.Yedekleme politikasının yerine getirilmesi için detaylı bir yedekleme analiz çalışması yapılmalı ve politikayı sağlayacak bir yedekleme planı ortaya koyulmalıdır. Yedekleme planının asgari aşağıdaki bilgileri içermesi gerekmektedir;

2.1.Yedekleme sıklığı,
2.2.Hangi saklama ortamında ne kadar süre tutulacağı,
2.3.Hangi yedekleme türü ile yedekleneceği,
2.4.Kabul edilebilir geri dönüş süresi,
2.5.Kabul edilebilir veri kaybı süresi.
2.6.Veri Analiz Çalışması
2.7.Yedekleme sistemi oluşturulmasının ilk adımı detaylı bir veri analiz çalışmasıdır.
2.8.Analiz çalışmalarında öncelikle kuruma ait veriler kategorize edilir.
2.9.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.
2.10.Kategorize edilen verilerin önem dereceleri bilgi güvenliği alt komisyonu tarafından belirlenir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Celal KÖSE Bilgi Güvenliği Yetkilisi	Kamil AKTAŞ Bilgi İşlem Sorumlusu-Uzman	Mehmet ŞAHİN Personel ve Destek Hizmetleri Başkanı

2.11.Kritik verilerin varlık envanteri özel önem gösterilmesi gereken bir hususdur. Bunun için kılavuzun A.13 (İş Sürekliliği Yönetimi) maddesi referans alınarak kritik varlık listesi oluşturulmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.
2.12.Oluşturulan varlık envanterinde hangi sistemlerde ne tür uygulamaların çalıştığı, yedeği alınacak dizin ve dosyalar, yetkili personel ve yetki seviyeleri yer almalıdır.
3.Yedekleme Listelerinin Oluşturulması
4.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.
5.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.
6.Yedeklenecek veriler bilgi işleme süreci içerisinde değişiklik gösterebileceğinden yedekleme listesi en az yılda 2 (iki) kez gözden geçirilmeli ve güncellenmelidir.
7.Yedekleme üniteleri üzerinde gereksiz yer ve lisans işgal edilmemesi için uygulama sahiplerinin yazılı onayı alınarak kritiklik düzeyi düşük olan ve sürekli büyüyen iz kaydı dosyaları yedekleme listesine dahil edilmemelidir.
8.Yedekleme listeleri kapasite yönetimi planlanması için referans oluşturur. Kapasite yönetimi ile ilgili hususlar kılavuzun A.9.3 maddesinde yer almaktadır.
9.Yedekleme Planlarının Oluşturulması
10.Başarılı bir yedekleme sistemi için kategorize edilmiş ve önceliklendirilmiş verilerin yedekleme planları oluşturulur.
11.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. Örnek bir Yedekleme Planı KLVZ-EK-14'da verilmiştir.
12.Kurumun gereklilikleri doğrultusunda hazırlanmış olan Yedekleme Planına göre yedeklerin düzenli aralıklarla alınması ve sürekli olarak gözden geçirilmesi gerekir.
13. Yedekleme Çalışmaları
14. 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.
15. Kritik olmayan veriler yedeklenirken, verilerin bir kopyası mevcut sunucular üzerinde, diğer bir kopyası çevrimdışı olarak yedekleme sunucusu veya harici depolama ortamlarında tutulur.
16. Yedekleme politikası ve planları doğrultusunda yapılan yedekleme işlemleri düzenli olarak kontrol edilmeli ve Yedekleme Kontrol Listesi ile kayıt altına alınmalıdır. Örnek bir Yedekleme Kontrol Listesi KLVZ-EK-15'de verilmiştir.
17. Kurumun yedekleme işlemlerinin başarısının ölçülmesi ve rapor oluşturulması amacıyla yedekleme başarısızlıkları izlenmeli ve kayıt altına alınmalıdır.
18. Özel nitelikli kişisel veri kategorisinde bulunan sağlık kayıtlarının yer aldığı yedekleme ortamları Kılavuzun A.7 (Kriptoloji) maddesinde yer alan usullerce şifrelenir.
19. Yedekleme medyaları acil durumlarda kullanılması gerekebileceğinden güvenilir ürünlerden seçilmeli ve düzenli periyotlarda test edilmelidir.
20. Yedekleme medyalarının bulundurulduğu ortamların fiziksel uygunluğu ve güvenliği sağlanmalı ve herhangi bir felaket anında etkilenmeyecek şekilde bilgi işlem odalarından farklı odalarda veya binalarda saklanmalıdır.
21. Geri Dönüş Testleri
22. Yedeklenen verilerin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için belirli aralıklarla geri dönüş testlerinin yapılması gerekir.
23. 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.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Celal KÖSE Bilgi Güvenliği Yetkilisi	Kamil AKTAŞ Bilgi İşlem Sorumlusu-Uzman	Mehmet ŞAHİN Personel ve Destek Hizmetleri Başkanı

24. Yedekten geri yükleme testlerinin, başarısız olması nedeniyle veri kaybı olabileceği durumu gözönüne alınarak, canlı ortamda değil gerçek ortamın aynısı olan test ortamında yapılması gerekmektedir.
25. Yedekleme Süreci Görev ve Sorumlulukları
26. Yedekleme politikasının işletilmesi ve zaman içerisinde günün ihtiyaçlarına göre güncellenmesi veri kaybı durumunda kurumun göreceği zararı en aza indirecektir.
27. Bu nedenle, yedekleme sistemlerinin yönetiminden, yedekleme politikasının ve yedekleme planının hazırlanmasından, uygulanmasından ve güncellenmesinden sorumlu personelin görevlendirilmesi gerekmektedir.
28. Yedekleme işleminin gerekli eğitimi almış personel tarafından yapılması sağlanmalıdır.
29. Teknik Açıklık Yönetimi
30. Açıklıkları gözleme, açıklık risk belirlemesi, yamalar, varlıkların izlenmesi, gerekli koordinasyon sorumlulukları dâhil teknik açıklıkların yönetimiyle ilgili görevler ve sorumluluklar belirlenmelidir.
31. Teknik açıklıkları belirlemek ve bunlarla ilgili farkındalığı sağlamak için kullanılacak kaynaklar varlık envanterinde belirtilmelidir. Bu kaynaklar envanter değişikliklerinde veya yeni kaynaklar bulunduğunda güncellenmelidir.
32. Yazılım/Donanım ürünlerinin çıkarmış olduğu yama ve/veya güncelleştirmeler periyodik olarak izlenmeli, bir güvenlik açığı riski veya bilgi güvenliği ihlali meydana gelmeden bu yama ve/veya güncelleştirmeler bütün sistemlere uygulanmalıdır.
33. Üreticiler tarafından yayımlanan yazılım/donanım yamaları mutlak suretle kontrol edilmeli, olumlu/olumsuz etkileri tespit edilmelidir. Yamaların mevcut sistemde farklı bir güvenlik açığı oluşturup oluşturmadığı tespit edilmeden, bu yamalar kullanıcılara dağıtılmamalıdır. Kullanılacak sürüm güncelleştirmeleri ya da yamalar için mutlaka "onaylanmış" / final sürüm olmasına dikkat edilmeli, test(beta) sürümlerinin sistemlere kurulmasından kaçınılmalıdır.
34. Potansiyel teknik açıklık bildirimlerine reaksiyon göstermek için bir zaman çizelgesi oluşturulmalıdır.
35. Yüksek riskli sistemler öncelikle belirlenmelidir.
36. Teknik açıklığın belirlenmesinin ardından konunun aciliyetine bağlı olarak alınması gereken önlemler müdahale öncesi yazılı olarak tanımlanmalı, tanımlanmış olan olay müdahale yönetimine uygun hareket edilmeli, risk içeren sistemler geçici olarak ağ bağlantısından çıkarılmalı, çıkarılamıyorsa mutlaka bir güvenlik duvarı arkasından minimum gereksinim ile hizmet verilmesine devam edilmelidir.
37. Bakanlık Sektörel SOME tarafından tespit edilen teknik açıklıklara dair henüz bir yama/güncelleme çıkmamış veya mevcut değilse, ilgili tedarikçi firma ile irtibata geçilerek söz konusu açıklığın kapatılması konusunda istek yapılmalıdır.
38. Uygulanan tüm prosedürler için denetim kaydı tutulmalıdır.
39. Açıklıklara ait bir risk derecelendirmesi olmalıdır. Derecelendirme sayısal olarak veya farklı renklendirme şeklinde yapılmalıdır. Risk derecelendirmesi, kuruluşun, risklerin giderilmesinde ve önceliklendirme yapılmasına imkân vermek üzere hazırlanmalıdır.
40. Kurumların SOME ve sistem yöneticileri koordinasyonu ile birlikte kurumun bilişim altyapısındaki kullanılan cihazlara izin verilen yazılım yüklemelerinin türü ve hangi tür yüklemelerin yasak olduğu belirlenir. Kullanıcılara yetki tanımlanırken en az ayrıcalık ilkesi uygulanmalı, yetkileri haricinde yazılım kurma hakkı tanımlanmamalıdır.
41. Kurumların bilişim altyapısında kullanılan cihazlara, lisanssız ya da güvenlik açığı yaratabilecek uygulamalar kurulmamalıdır.
42. Bilgisayarlara ağ trafiğini gereksiz yere meşgul edebilecek p2p,torrent gibi her türlü dosya paylaşım yazılımlarının kurulmaları engellenmelidir.
43. Sistem Güvenlik Testleri
43.1. Yıllık plan yapılmalı, bu plan ile takvim günleri belirlenmelidir.
43.2. Yapılacak kontroller ve testler ISO 27001 sistemine, TÜBİTAK UEKAE, TS 13638 ve Siber Güvenlik Enstitüsü standartlarına bağlı kalınarak yürütülmelidir.
43.3. Güvenlik testleri, konusunda uzman/yetkin sertifikalı personeller tarafından yapılır.

43.4. Yapılacak Güvenlik Testleri üst yönetim tarafından onay alındıktan sonra, ilgili kuruluşa önceden haber verilip gerekli izinler sağlandıktan sonra gerçekleştirilir.
43.5. Yapılacak Sızma testleri kapsamında alınması gereken ayrıcalıklı erişimler talep edilir. Ayrıcalıklı erişim talep eden kişiye ait IP ve MAC adresi bilgileri mutlaka belirtilmelidir.
43.6. Yapılacak güvenlik testleri kapsamı en az aşağıdaki test adımlarından oluşur;
43.6.1. Ağ ve Sistem Altyapısı Sızma Testi
43.6.2. Yerel ağ sızma testleri
43.6.3. İnternet üzerinden sızma testleri
43.6.4. Güvenlik Sistemleri (Antivirüs, IPS/IDS, Güvenlik Duvarı vb.) Sızma testleri
43.6.5. İşletim Sistemleri
43.6.6. Kablosuz Ağ Sızma Testi
43.6.7. Web Uygulama Sızma Testi
43.6.8. Mobil Uygulama Sızma Testi
43.6.9. Veri Tabanı Testleri
43.6.10. Hizmet Aksatma Saldırı (DoS/DDOS) Testleri
43.6.11. Sosyal Mühendislik Testleri
44. Yapılan testler sonucunda ortaya çıkan sonuçlar önem derecesine göre raporlanmalıdır. Bu raporların oluşturulmasında TS 13638 standart raporlama örneği temel alınarak yapılmalıdır.
45. Oluşturulan Bilgi Güvenliği Analiz Raporu, Bilgi Güvenliği Yönetim Komisyonu tarafından değerlendirilerek Acil Eylem Planı oluşturulur ve açıklıkların kapatılması için çalışmalar başlatılır.
46. Ortaya çıkan zafiyetler sonucunda alınacak önlemler kapsamında, ilgili kuruluşun Kurumsal SOME'si tarafından konfigürasyon ayarları, sistem ve ağ topolojisi kontrol edilmeli ve gereken önlemler alınması için çalışma yapılır.
47. Yapılan çalışmalar sonucunda ortaya çıkan sonuç Bilgi Güvenliği Komisyonuna sunulur. Kapatılamayan zafiyetler risk tablosunu işlenir.
48. Raporlar şifreli ortamda ve gizli sıfatıyla tutulmalıdır. Rapor içeriğindeki ilgili bölümlerin önceliklendirme seviyesine göre gerekli hallerde ek farkındalık eğitimleri, seminerler verilmelidir.
49. Siber saldırıların önlemesi faaliyetleri kapsamında Zafiyet/Açıklık ve Sosyal Mühendislik testlerini Bakanlık Merkez ve Merkeze bağlı kuruluşlarda, Taşra teşkilatlarımızda Bakanlığımızın SBSGM Bünyesinde bulunan Sektörel SOME tarafından uzak sunucu vasıtasıyla gerçekleştirilmesiyle yapılır.
50. Güvenlik testleri ve Kaynak Kod Analizi, geliştirilecek olan yazılımlara ait şartnamelerde yer almalıdır. A.9.15.14. Kaynak kod analizi, KLVZ-EK-13 Güvenli Yazılım Geliştirme Kontrol Listesinde yer alan kriterler kullanılmak suretiyle gerçekleştirilir.