T.C.
DENİZLİ VALİLİĞİ
İL SAĞLIK MÜDÜRLÜĞÜ
BİLGİ SAKLAMA ORTAMLARI YOK ETME PROSEDÜRÜ

1. AMAÇ
Müdürlüğümüz ve Bağlı Sağlık Tesisleri bünyesindeki basılı ortamlar ve bilgi işlem cihazları da dahil her türlü ortamda saklanan bilgilerin silinmesi, anonim hale getirilmesi ve imha edilmesi ile ilgili hususları açıklamak

2. KAPSAM
Denizli İl Sağlık Müdürlüğü Bilgi Güvenliği Yönetim Sistemi Politika metninde yer alan kapsam maddesinde belirlenmiş olan kapsamdır.

3. TANIMLAR
İSM: Denizli İl Sağlık Müdürlüğü

4. SORUMLULUKLAR
Bu prosedürün uygulanmasından ilgili kurum yöneticileri sorumludur.

5. UYGULAMA
5.1. Bilgi Saklama Ortamları Yok Etme Prosedürü
5.1.1. Kullanılan bilgi kaynaklarının yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır

5.1.2. Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik veya fiziki nedenlerle kullanılmasında yarar görülmeyerek hizmet dışı bırakılmasına karar verilen bilgi sistem cihazları ile ilgili kayıt silme işlemleri 2006/11545 sayılı Taşınır Mal Yönetmeliğinde belirtilen usul ve esaslar çerçevesince, ilgili birimler ve komisyonlar tarafında yapılır.

5.1.3. Kaydı silinen bilgi sistem cihazlarına ait veri depolama üniteleri, içerisinde gizlilik dereceli bilgi bulundurma ihtimali nedeniyle usulüne uygun olarak imha edilir veya güvenli silme işlemi yapılır.

5.1.4. Kaydı silinen bilgisayarların sabit diskleri, ilgili teknik birimlerden destek alınmak suretiyle sökülür.

5.1.5. Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.

5.1.6. İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.

5.1.7. Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.

5.1.8. Yetkilendirilmiş personel tarafından imhası gerçekleşen veri depolama üniteleri için ürünlerin seri numaraları ve adet bilgisini içerecek şekilde **"Disk İmha Formu"** doldurulmalı ve imza altına alınmalıdır.

5.1.9. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.

5.1.10. Tamamen tahrip edilememiş disk parçalarının delme, kesme makineleri ile kullanılamaz hale getirilmelidir.

5.1.11. Hacimsel küçültme işlemi için parçalanmalıdır.

Hazırlayanlar	Kontrol Eden	Onaylayan

5.1.12. Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.
5.1.13. Yeniden kullanılması planlanan disklere, içlerinde yer alan bilgilerin yetkisiz kişilerin eline geçmesini engellemek maksadıyla 'güvenli sil' (üzerine yazma) işlemi yapılır.
5.1.14. Güvenli silme işlemi, manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu iş için uygun bir yazılım (DBAN, Kill Disk, Eraser, Disk Wipe, HDShredder gibi) veya donanım kullanılır.
5.1.15. Arızalanan ya da bakıma gönderilen cihazlarda yer alan hassas verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:
5.1.16. İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan veriler güvenli olarak silinmelidir,
5.1.17. Güvenli silmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
5.1.18. Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, hassas verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

6. YAPTIRIM

Bu prosedürün ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla BGYS Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

Hazırlayanlar	Kontrol Eden	Onaylayan