


 T.C. Sağlık Bakanlığı	<b>GİRESUN İL SAĞLIK MÜDÜRLÜĞÜ</b> <b>BİLGİ SAKLAMA ORTAMLARI YOK ETME</b> <b>PROSEDÜRÜ</b>			 T.C. Sağlık Bakanlığı Giresun İl Sağlık Müdürlüğü
<b>Kodu</b>	<b>Yayınlama tarihi</b>	<b>Revizyon Tarihi</b>	<b>Revizyon No</b>	<b>Sayfa</b>
<b>BG.PO.01</b>				<b>1/2</b>

Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik veya fiziki nedenlerle kullanılmasında yarar görülmemekle birlikte 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 tarafından yapılır.

1. 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.
2. Kaydı silinen bilgisayarların sabit diskleri, ilgili teknik birimlerden destek alınmak suretiyle sökülür.
3. Sökülen sabit disklerden daha önce ilgili teknik birimler tarafından “onarımı mümkün değil” şeklinde rapor verilenler ile sağlam olmakla birlikte “yeniden kullanımı düşünülmeyen” cihazlar aşağıda belirtilen yöntemlerden biri ya da birkaçı birlikte kullanılmak suretiyle imha edilir.
4. De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
5. Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.
6. Sabit disklerin fiziksel imha işlemlerinin standartlara uygun şekilde yürütülmesi amacıyla Sağlık Bilgi Sistemleri Genel Müdürlüğünde bulunan disk imha cihazı kullanılabilir. Disk imhası için imha edilecek diskler için Kayıttan Düşme Teklif ve Onay Tutanağı (KLVZ-EK-03) ve Disk İmha Formunun (KLVZ-EK-04) resmi yazı ile Genel Müdürlüğe gönderilmesi gerekir. Disk imha işlemleri, bizzat disklerin sahipleri veya taşınır mal sorumlularının nezaretinde yapılır.
7. Bilgisayarların sabit diskleri dışında hassas veri bulundurma ihtimali olan diğer depolama ortamları, ortam türüne bağlı olarak aşağıda yer alan yöntemlerden biri kullanılarak yok edilir.
  - 7.1. Ağ cihazları (anahtarlama cihazı, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
  - 7.2. Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanarak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemi ile ya da Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
  - 7.3. Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp demanyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.
  - 7.4. Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.
  - 7.5. Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
  - 7.6. Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.
  - 7.7. Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

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

 T.C. Sağlık Bakanlığı	<b>GİRESUN İL SAĞLIK MÜDÜRLÜĞÜ</b> <b>BİLGİ SAKLAMA ORTAMLARI YOK ETME</b> <b>PROSEDÜRÜ</b>			 T.C. Sağlık Bakanlığı Giresun İl Sağlık Müdürlüğü
<b>Kodu</b>	<b>Yayınlama tarihi</b>	<b>Revizyon Tarihi</b>	<b>Revizyon No</b>	<b>Sayfa</b>
<b>BG.PO.01</b>				<b>2/2</b>

**7.8.** Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

**7.9.** Kağıt ve mikrofiş ortamlarındaki veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

**7.10.** Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

**7.11.** Yeniden kullanılması planlanan disklerle, içlerinde yer alan bilgilerin yetkisiz kişilerin eline geçmesini engellemek amacıyla, güvenli sil (üzerine yazma) işlemi yapılır.

**7.12.** 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.

**7.13.** Bulut ortamındaki sistemlerde yer alan hassas verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılamaz hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

**7.14.** Arızalanan ya da bakıma gönderilen cihazlarda yer alan hassas verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

**7.14.1.** İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan verilerin Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

**7.14.2.** Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

**7.14.3.** Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, hassas verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

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