



BİLGİ SAKLAMA ORTAMLARI YOK ETME PROSEDÜRÜ

Kodu
BG.PR.02

Yayınlanma Tarihi
25/10/2018

Revizyon Tarihi

Revizyon No

Sayfa
1 / 2

1. AMAÇ

T.C. Sağlık Bakanlığı Düzce İl Sağlık Müdürlüğü ve bağlı sağlık tesisleri bünyesinde bilgi saklama ortamlarının nasıl yok edileceğini belirlemektir.

2. KAPSAM

T.C. Sağlık Bakanlığı Düzce İl Sağlık Müdürlüğü'ne ait bütün bilgi varlıklarını kapsar.

3. PROSEDÜR METNİ

3.1. Yasal bekleme süreleri sonunda evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırılma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.

3.2. 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.

3.3. 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:

3.3.1. De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

3.3.2. Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optikveya 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.

3.3.3. Bilgisayarların sabit diskleri dışında hassas veri bulundurma ihtimali olan diğer depolama ortamları, ortam türüne bağlı olarak aşağıda yer alan yöntemlerden biri kullanılarak yok edilir.

3.3.3.1. Ağ cihazları (anahtarlar, cihaz, yönlendirici vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Madde 3.3. de yer alan uygun yöneteme göre yok edilir.

3.3.3.2. Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <blockerase> komutunu kullanarak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemiyle ya da Madde 3.3. de yer alan uygun yöneteme göre yok edilir.

3.3.3.3. Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatis 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.

3.3.3.4. Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatis 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.

3.3.3.5. Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta ancak çoğunda yok etme komutu bulunmamaktadır. Madde 3.3. de yer alan uygun yöneteme göre yok edilir.

3.3.3.6. Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

3.3.3.7. Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre madde 3.3. de yer alan uygun yöneteme göre yok edilir.

3.3.3.8. Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu



BİLGİ SAKLAMA ORTAMLARI YOK ETME PROSEDÜRÜ

Kodu
BG.PR.02

Yayınlanma Tarihi
25/10/2018

Revizyon Tarihi

Revizyon No

Sayfa
2 / 2

sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. Madde 3.3. de yer alan uygun yöneteme göre yok edilir.

- 3.4.** Kâğıt ve mikrofiş ortamlarındaki veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kâğıt imha veya kırılma makineleri ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
- 3.5.** Orijinal kâğıt formattan tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre madde 3.3. de yer alan uygun yöneteme göre yok edilir.
- 3.6.** Yeniden kullanılması planlanan disklerle, içlerinde yer alan bilgilerin yetkisiz kişilerin eline geçmesini engellemek amacıyla 'güvenli sil' (üzerine yazma) işlemi yapılır. 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, HDS shredder gibi) veya donanım kullanılır.
- 3.7.** 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.
- 3.8.** Arızalanan ya da bakıma gönderilen cihazlarda yer alan hassas verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:
 - 3.8.1.** İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan veriler madde 3.3. de yer alan uygun yöneteme göre yok edilir.
 - 3.8.2.** Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamı sökülerek saklanır, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilir.
 - 3.8.3.** Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, hassas verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.