	DATA İMHA POLİTİKASI	Doküman No	PO.017
		Yayın Tarihi	01.07.2024
		Revizyon No	00
		Revizyon Tarihi	
		Toplam Sayfa Sayısı	16

1. AMAÇ: Bu politikanın amacı, EGE Üniversitesi Hastanesi (Sağlık Uygulama ve Araştırma Merkezi) kurumundaki kritik bilgilerin yetkisiz kişilere sızmasını engellemek için gerekli görülen durumlarda bilginin taşındığı ve saklandığı ortamların imhası veya okunamaz hale getirilmesi işlemleri ile ilgili kuralları tanımlamaktır.

2. KAPSAM: Bu politika kuruma bağlı imha edilmesine karar verilen kritik bilgi varlıklarını kapsamaktadır.

3. SORUMLULUK

3.1. Bilgi İşlem Daire Başkanlığı (BİDB) Üst Yönetim: Politikanın uygulanması için gerekli gözetimin sağlanmasından sorumlu olan kişidir.

3.2. Bilgi Güvenliği Yönetim Sistemi (BGYS) Ekibi: Politikanın Üst Yönetim desteğinin sağlanmasından, tüm iş birimleri tarafından anlaşılıp desteklenmesinden ve etkin şekilde uygulanmasından sorumludur.

3.3. Sistem Yöneticisi: Politikanın gereklerinin görev alanlarının gerektirdiği biçimde uygulanmasından sorumludur.

4. UYGULAMA

4.1. KÂĞIT ORTAM

4.1.1. Sistem Yöneticisi **"Kayıtların Kontrolü Prosedürü"** ne göre saklama süresi dolan kayıtları ilgili bölüm yöneticisinin belirlediği yöntemle imha edilir.

4.1.2. BGYS dokümantasyonu tarafındaki imha edilecek dokumanlar BGYS Ekibibilgisi dahilinde yapılır.

4.2. Elektronik Ortam

4.2.1. Sistem Yöneticisi **"Kayıtların Kontrolü Prosedürü"** ne göre saklama süresi dolan kayıtları kağıt öğütücü ile imha edilir.

4.2.2. Elektronik ortamda kullanımı biten kritik önem taşıyan bilgiler Sistem Yöneticisinin belirlediği yöntemle silinecektir.

4.2.3. Sistem Yöneticisinin gerekli gördüğü durumlarda kritik bilgiyi taşıyan ortamlar fiziksel olarak bir araya getirilemeyecek şekilde imha edilecektir.

4.2.4. İmha edilecek ortamların sayısına göre Sistem Yöneticisinin kararı ile BİDB Personeli, dataları aşağıdaki güvenli silme işlemlerinde sonra hurda haline getirilerek Devletin belirlediği yetkili imha kuruluşuna teslim edilir.

4.2.5. Sabit Disk ve Yazılabilir Taşınabilir Ortam Güvenli Silme

Bu süreç için uygun yazılım kullanılır ve diskler geri dönüşsüz silinir.

4.2.6. Çok Gizli Verilerin Temizlenmesi İçin

Gizlilik seviyesi yüksek olduğu durumlarda buna uygun olarak belirlenen bitlerin yazılmasının da içeren çok

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

defa tüm diskin yazılması yöntemi kullanılmalıdır.
Gerekli durumlarda gizli bilgi barındıran ortamların imhasında fiziksel imha yöntemleri de (kırma, yakma, v.s.) kullanılabilir.

4.2.7. El Cihazları İçin Güvenli Silme Prosedürü

İçinde ulusal güvenlik sorunu oluşturacak türde bilgiler barındırmayan el cihazları için "hard reset - PDA'ler için" gibi cihazların sağladığı fonksiyonlar kullanılır. Çok kritik bilgi barındıran el cihazları ya fiziksel olarak imha edilir ya da bu cihazlara özel olarak geliştirilmiş güvenlik yazılımları kullanılarak güvenli silme yapılır (ör: Paraben).

4.2.8. Ağ Cihazları İçin Güvenli Silme Prosedürü

Ağ cihazları atılmadan, satılmadan veya hibe edilmeden önce üzerlerindeki konfigürasyon silinir. Bunun için cihaza özel komut ve yöntemler kullanılır (ör: Cisco cihazları için "write erase" komutu bu amaçla kullanılır). İlgili cihaz için güvenli silme prosedür detayları için üretici dokümantasyonu veya çevrimiçi kaynaklara bakılmalıdır.

5. YAPTIRIM

5.1. Bu politikaya ve ilgili süreçlere uygun olarak çalışmayan tüm personel hakkında "**Disiplin Prosedürü**" hükümleri uygulanır.

6. İLGİLİ DOKÜMANLAR

6.1. Disiplin Prosedürü
6.2. Kayıtların Kontrolü Prosedürü

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı