# AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde arızalanmış, teknik ömrünü tamamlamış, gelişen teknolojinin gerisinde kalmış BT varlıklarının güvenli ve düzenli bir şekilde imha edilmesi amacıyla hazırlanmıştır.

# DAYANAK

Bu prosedür,

1. 2019/12 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi,
2. T.C. Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi,
3. Kamu İç Kontrol Standartları Tebliği’nin “Bilgi Sistemleri Kontrolleri” başlıklı 12 numaralı Standardına dayanılarak hazırlanmıştır.

# KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından yönetilen aşağıda yer alan BT varlıklarını kapsar.

* Bilgisayarlar (masaüstü, dizüstü)
* Sunucular
* Veri depolama üniteleri

# SORUMLULAR

* **Bilgi İşlem Daire Başkanı**: Bu prosedürün denetlenmesinden ve imha denetim formunun doldurulmasından sorumludur.
* **Varlık Sahipleri**: İmha edilecek BT varlıklarının İmha Feragat Formu ile Bilgi İşlem Daire Başkanlığına bildirilmesinden sorumludur.
* **İmha Komisyonu**: BT varlıklarının güvenli bir şekilde imha edilmesine ilişkin kararların alınmasından ve uygulanmasından sorumludur.

# KISALTMALAR VE TANIMLAR

**BT:** Bilgi Teknolojileri

**BİDB:** Bilgi İşlem Daire Başkanlığı

**KMÜ:** Karamanoğlu Mehmetbey Üniversitesi

**SSD:** Solid State Drive (Katı Hal Sürücüsü)

**BT Varlıkları**: Bilgi teknolojileri kapsamında kullanılan, bu prosedür kapsamındaki tüm donanım ve yazılım bileşenleridir.

# VERİ GÜVENLİĞİ

**Veri Yedekleme**: Kullanımdan çıkartılacak BT varlıklarında bulunan veriler, gerekiyorsa uygun bir ortamda yedeklenir.

**Veri Silme**: BT varlıkları üzerindeki tüm veriler, güvenli veri silme yöntemleri kullanılarak kalıcı olarak silinir.

**Disk Yok Etme**: Veri depolama ünitelerinin disk kısımları fiziksel olarak tahrip edilir.

# KURUM DIŞI ONARIM GÖRECEK CİHAZLAR

Onarım/tadilat için üçüncü kişilere (yetkili servis vb.) verilecek cihazların disk arızası yok ise veri depolama üniteleri sökülüp gönderilir. Disk arızası olduğu durumda ise verinin güvenliği açısından diskte kritik bilgilerin olduğu öngörülüyorsa disk tamir için dışarıya gönderilmeyecek ve yeni disk verilerek kullanıcının varsa yedekleri sistemden dönülerek yeni diske aktarılacaktır. Disk, içinde bulunan verilerin yedeği yoksa ve hizmet alımı
yöntemiyle kurtarılması ihtimali varsa hizmet verecek tamir servisi ile
gizlilik sözleşmesi imzalandıktan sonra gönderilecektir.

# UYGULAMA

## Değerlendirme

İmha Komisyonu, bildirilen BT varlıklarını inceler ve değerlendirir. Değerlendirme sonucunda imha kararını tutanakla kayıt altına alır.

## İmha ve Bertaraf

### İmha Yöntemleri

**Fiziksel İmha**: Kullanım ömrünü tamamlamış BT varlıkları, İmha Komisyonu üyeleri gözetiminde fiziksel olarak tahrip edilir.

**Bağış ve Yeniden Kullanım:** Kullanılabilir durumda olan BT varlıkları, uygun görülen kurum veya kuruluşlara bağışlanabilir veya üniversite bünyesinde farklı bir amaçla kullanılabilir. Bu diskler güvenli veri silme yöntemi uygulandıktan sonra bağışlanabilir veya kurum içinde yeniden kullanıma sunulabilir.

**Güvenli Veri Silme Yöntemleri:**

1. **Yazılımsal Veri Silme (Software-Based Data Erasure):** Verinin üzerine bir veya daha fazla kez rastgele veri veya belirli bir desenle yazılarak orijinal verinin geri döndürülemez şekilde silinmesi sağlanır. Bu yöntem, genellikle "overwrite" (üzerine yazma) olarak da bilinir.
2. **Donanımsal Veri Silme (Hardware-Based Data Erasure):** Sabit disk veya diğer depolama birimlerinin yerleşik özellikleri kullanılarak yapılan silme işlemleridir. Örneğin modern sabit disklerin ve SSD'lerin çoğu, tüm depolama alanını kalıcı olarak silmek için yerleşik bir komut (örneğin "Secure Erase") sunar.
3. **Manyetik Silme (Degaussing):** Manyetik depolama birimlerinin (örneğin manyetik diskler veya manyetik bantlar) üzerindeki verilerin bir manyetik alan yardımıyla silinmesidir. Bu yöntem, manyetik ortamdaki veriyi okunamaz hale getirir ve genellikle fiziksel imha ile kullanılır.

### İmha İşleminin Kayıt Altına Alınması

İmha işlemleri, İmha Komisyonu tarafından yazılı ve görsel olarak kayıt altına alınır.

## Denetim

Kullanımdan Çıkartılacak veya İmha Edilecek BT Varlıkları Prosedürü’nün etkin bir şekilde uygulanmasını sağlamak amacıyla düzenli denetimler yapılır.

## Gizlilik ve Güvenlik

İmha işlemleri sırasında veri gizliliği ve güvenliği en üst düzeyde tutulur. İmha işlemleri, yetkili personel tarafından ve güvenli ortamlarda gerçekleştirilir.

## Eğitim ve Farkındalık

BİDB personeli, İmha Komisyonu tarafından BT varlıkları imha prosedürleri hakkında düzenli olarak eğitilir ve farkındalık çalışmaları yapılır.

## Revizyon

Bu prosedür, BİDB tarafından ihtiyaçlar doğrultusunda periyodik olarak gözden geçirilir ve güncellenir.

# KOMİSYONLAR

## İmha Komisyonunun Oluşturulması

KMÜ BİDB’de yapılacak imha işlemleri için Bilgi İşlem Daire Başkanının başkanlığında Şube Müdürü, Sistem Yönetim Birimi Sorumlusu, Taşınır Kayıt Yetkilisi, Teknik Hizmetler ve Donanım Birimi Sorumlusu olmak üzere dört kişilik bir İmha Komisyonu kurulur.

# İLGİLİ DOKÜMANLAR

* Kişisel Veri Saklama ve İmha Politikası
* Varlık Yönetimi Politikası
* Fiziksel ve Çevresel Güvenlik Politikası
* Yedekleme ve Kurtarma Politikası
* İmha Feragat Formu
* Gizlilik Sözleşmesi