

1. AMAÇ

Bu prosedürün amacı, Bursa Uludağ Üniversitesi bünyesindeki Bilgi İşlem Daire Başkanlığı kapsamında veri saklanan bilişim sistemlerinin (harddisk, cd, usb, vb.) veri imha yöntemlerini belirlemektir.

2. KAPSAM

Bu prosedür;

- Elektronik ortamlar (sunucu, bilgisayar, taşınabilir disk, bulut sistemleri),
- Fiziksel dokümanlar (kâğıt ortamları),
- Optik ve manyetik medya (DVD, USB, tape yedekleri),
- Donanımlar ve bilgi içeren tüm varlıklar üzerindeki veri imha süreçlerini kapsar.

Tüm çalışanlar, taşeronlar ve üçüncü taraflar bu prosedüre uymakla yükümlüdür.

3. SORUMLULUKLAR

Bilgi Güvenliği Yöneticisi: Prosedürün uygulanmasını denetler.

Sistem Yöneticileri: Elektronik ortamların güvenli silinmesinden sorumludur.

Arşiv Sorumluları: Fiziksel dokümanların güvenli imhasından sorumludur.

Varlık Sahipleri: İmha edilmesi gereken varlığı belirleyip talepte bulunur.

Üçüncü Taraflar: İmha sürecinde kalite ve gizlilik sözleşmelerine uyar.

4. TANIMLAR

İmha : Veri saklanan bilişim sistemlerinin (harddisk, cd, usb, vb.) içindeki bilgilerin erişilemez hale getirilmesidir.

Kişisel Veri : Üniversitemizin KVKK bilgilendirme sayfasında yayınlanmaktadır.

5. UYGULAMA

4.1 Varlıkların İmhası

Bilgi kayıt özelliğine sahip her türlü cihazın üzerindeki bilgiler yetkisiz erişime karşı silinir ve cihaz üzerindeki disk ve kayıt mekanizması fiziksel olarak tahrip edilir.

4.2 Verilerin Silinmesi Yöntemleri

- a. Kâğıt Ortamında Bulunan Kişisel Veriler: Kâğıt öğütücü ile imha edilerek ya da gerekli durumlarda karartma yöntemi kullanılarak silinmektedir.
- b. İşletim sistemindeki silme komutu ile silinir.
- c. Kalıcı biçimlendirme ile veriler ulaşılamaz hale getirilir.
- d. Veri Tabanları: Verilerin bulunduğu ilgili satırlar veri tabanı komutları ile silinir.

4.3 Varlıkların ve Verinin Yok Edilmesi Yöntemleri

- a. Yerel Sistemlerde: De-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerinden uygun olanı kullanılarak yok edilir.
- b. Çevresel Sistemler:
- Ağ cihazları (switch, router vb.): a maddesinde belirtilen uygun yöntemler ile yok edilir.
 - Flash tabanlı ortamlar: İlgili üreticinin önerdiği yöntemler ya da a maddesinde belirtilen yöntemler ile yok edilir.
 - Manyetik bant: De-manyetize ederek ya da yakma, eritme gibi fiziksel yöntemlerle yok edilir.
 - Sim Kart ve sabit hafıza kartları: a maddesinde de belirtilen uygun yöntemler ile yok edilir.
 - Optik diskler: yakma, küçük parçalara ayırma, eritme gibi fiziksel yöntemlerle yok edilir.
 - Veri Kayıt Ortamı sabit olan çevre birimleri: a maddesinde belirtilen uygun yöntemler ile yok edilir.
- c. Basılı Ortamlar: Kâğıt imha makinaları kullanılarak yok edilir. Orijinal kâğıt formattan tarama yoluyla elektronik ortama aktarılan Kişisel veriler ise bulundukları ortama göre uygun yöntemlerle yok edilirler.
- İçerisindeki veriler temizlenen bilişim varlıkları FR 3.2.3_05 Hurda ve kayıp bildirim formu ile Uludağ Üniversitesi Merkezi Hurda Deposuna teslim edilir.

4.4 Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri:

Üniversitemizin KVKK bilgilendirme sayfasında yayınlanmaktadır.

4.5 Veri Sahibi Talebi Üzerine Kişisel Kullanıcı Hesabının Kaldırılması

BURSA ULUDAĞ ÜNİVERSİTESİ BİLGİSAYAR, AĞ VE BİLİŞİM KAYNAKLARI KULLANIM YÖNERGESİ'nde açıklanmıştır.

4.6 Kişisel Verilerin Periyodik Gözden Geçirmesi

Kişisel Verilerin Korunması hakkındaki kanun ve 5651 sayılı kanun hükümlerine göre işlem yapılmaktadır.

4.7 Kişisel Verilerin Saklanması

BURSA ULUDAĞ ÜNİVERSİTESİ BİLGİSAYAR, AĞ VE BİLİŞİM KAYNAKLARI KULLANIM YÖNERGESİ'nde açıklanmıştır.

Kişisel Verilerin Korunması hakkındaki kanun ve 5651 sayılı kanun hükümlerine göre işlem yapılmaktadır.

5. REFERANSLAR:

6698 Sayılı Kişisel Verilerin Korunması Kanunun 30224 Sayılı 28.10.2018 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik