	TNKÜ **DATA İMHA POLİTİKASI**	Doküman No:	EYS-PO-031
		Hazırlama Tarihi:	14.08.2025
		Revizyon Tarihi:	--
		Revizyon No:	0
		Toplam Sayfa Sayısı:	2

1 AMAÇ

Bu politikanın amacı, Tekirdağ Namık Kemal Üniversitesi 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

Tekirdağ Namık Kemal Üniversitesi bünyesinde görev alan ve hassas bilgilere erişebilen tüm personeli kapsar.

3 SORUMLULAR

Bu politikanın oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Politikanın uygulanmasından hassas bilgilere erişebilen tüm Tekirdağ Namık Kemal Üniversitesi personeli sorumludur.

Kurallar

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 Ekibi bilgisi 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 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, izin verilemez.

5 YAPTIRIM

Bu politikanın ihlal edilmesi durumunda Disiplin Prosedürü uygulanacaktır.

6 İLGİLİ DOKÜMANLAR

EYS-PR.021 - DİSİPLİN PROSEDÜRÜ