1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında kullanılan basılı ve elektronik bilgi ortamlarının kullanım ömrünün sona ermesi, ihtiyaç duyulmaması, yeniden kullanım veya elden çıkarma süreçlerinde üzerinde bulunan bilgilerin yetkisiz kişiler tarafından elde edilmesini, kullanılmasını, değiştirilmesini veya ifşa edilmesini önlemek ve bilgi varlıklarının güvenli şekilde imha edilmesine ilişkin kuralları belirlemektir.

Politika kapsamında özellikle kişisel veriler, özel nitelikli kişisel veriler, gizli bilgiler, kritik bilgiler ve bilgi güvenliği açısından hassas verilerin imha edilmesi sırasında bilgi güvenliği ve kişisel verilerin korunması ilkeleri esas alınır.

2. KAPSAM

Bu politika;

- Süleyman Demirel Üniversitesi Daire Başkanlıklarını,
- Genel Sekreterliği,
- Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimini,
- Bu birimlerde kullanılan bilgi ve bilgi varlıklarını,
- Basılı dokümanları,
- CD/DVD ve benzeri optik ortamları,
- USB bellekleri,
- Taşınabilir diskleri,
- Bilgisayar ve sunucu disklerini,
- Yedekleme ortamlarını ve kartuşları,
- Bellek kartlarını,
- Mobil cihazlarda bulunan veri depolama ortamlarını,
- Sanal diskleri ve sanal makine disklerini,
- Bilginin depolandığı ve kullanım ömrü sona eren diğer elektronik ortamları kapsar.

İmha işlemlerinde ilgili saklama süreleri, arşiv mevzuatı, kişisel veri saklama ve imha süreçleri, hukuki yükümlülükler ve bilgi varlığı sahibi tarafından belirlenen gereklilikler dikkate alınır.

3. SORUMLULUKLAR

3.1. Birim Yöneticileri

- İmha edilmesi gereken bilgi ve ortamların belirlenmesini,
- İmha işleminin yetkili kişilerce gerçekleştirilmesini,
- Gerekli durumlarda imha komisyonu veya yetkili personelin görevlendirilmesini,
- İmha kayıtlarının tutulmasını,
- İmha işleminin ilgili mevzuat ve EYS dokümanlarına uygun yürütülmesini sağlar.

3.2. Bilgi Varlığı Sahipleri

Bilgi varlığı sahipleri, ilgili bilgi varlığının saklama süresinin sona ermesi veya imha şartlarının oluşması durumunda imha ihtiyacını belirler ve gerekli onay/işlemlerin başlatılmasını sağlar.

3.3. Bilgi İşlem Daire Başkanlığı

BİDB, sorumluluğundaki bilgi sistemleri ve elektronik ortamların güvenli silinmesi, yeniden kullanım veya imha süreçlerinde teknik desteği sağlar.

3.4. Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi

Hastane Bilgi İşlem Birimi, sorumluluğundaki sunucu, bilgisayar, depolama ortamı ve diğer elektronik bilgi varlıklarında bulunan verilerin güvenli şekilde silinmesi veya imha edilmesine ilişkin teknik işlemleri yürütür.

Hasta ve sağlık verisi içeren bilgi ortamlarının imhasında kişisel verilerin ve özel nitelikli kişisel verilerin korunmasına ilişkin kurallar ayrıca dikkate alınır.

3.5. Tüm Personel

- İmha edilmesi gereken bilgi ve ortamları yetkisiz kişilere teslim etmemek,
- İmha edilmemiş bilgi içeren ortamları çöpe atmamak,
- Kurum dışına çıkarmamak,
- Yetkisiz kişilere vermemek,
- İmha işlemini kendi yetkisi dışında gerçekleştirmemek,
- İmha edilmesi gereken ortamları ilgili birime teslim etmek ile sorumludur.

4. UYGULAMA

4.1. İmha Öncesi Kontroller

İmha işlemi gerçekleştirilmeden önce;

1. Bilgi veya ortamın saklama süresinin sona erip ermediği,
2. Arşivlenmesi veya saklanması gerekip gerekmediği,
3. Devam eden bir hukuki, idari veya denetim sürecinde delil niteliği taşıyıp taşımadığı,
4. Bilgi varlığının başka bir sistemde veya ortamda tutulmasının gerekip gerekmediği,
5. Kişisel veri veya özel nitelikli kişisel veri içerip içermediği,
6. Bilgi sınıflandırmasının ne olduğu,
7. Yeniden kullanım veya devrin mümkün olup olmadığı değerlendirilir.
8. Devam eden hukuki, idari, mali, denetim veya benzeri bir süreçte kullanılması gereken bilgi ve ortamlar ilgili süreç sonuçlanmadan imha edilmez.

4.2. Basılı Ortamların İmhası

1. Saklama süresi sona eren ve arşivlenmesine gerek bulunmayan basılı bilgi varlıkları güvenli şekilde imha edilir.
2. Hizmete Özel, Gizli, Çok Gizli, kişisel veri veya özel nitelikli kişisel veri içeren belgeler normal atık veya geri dönüşüm kutularına bırakılmaz.
3. Bu tür belgeler, içeriğin okunamayacak ve yeniden oluşturulamayacak hale gelmesini sağlayacak yöntemlerle imha edilir.
4. İmha işlemi kurumun imkânlarına göre;
    - Güvenli evrak imha makinesi,
    - Kırpma/parçalama,
    - Yetkilendirilmiş güvenli imha hizmeti gibi uygun yöntemlerle gerçekleştirilebilir.

5. Toplu imha işlemlerinde gerektiğinde imha tutanağı düzenlenir.

4.3. Elektronik Ortamların İmhası

Aşağıdaki elektronik ortamlar üzerinde bulunan bilgiler, ortamın yeniden kullanılması veya elden çıkarılması öncesinde güvenli şekilde silinir veya imha edilir:

- USB bellekler,
- Taşınabilir diskler,
- HDD,
- SSD,
- CD/DVD,
- Bellek kartları,
- Bilgisayar diskleri,
- Sunucu diskleri,
- Yedekleme ortamları,
- Kartuşlar,
- Diğer veri depolama ortamları.

4.3.1. Güvenli Silme

Elektronik ortam yeniden kullanılacaksa veya fiziksel olarak imha edilmeyecekse, üzerinde bulunan verilerin yetkisiz araçlarla geri getirilemeyecek şekilde silinmesi sağlanır. Silme işlemi, kullanılan depolama teknolojisinin özelliklerine uygun güvenli silme yöntemleri kullanılarak gerçekleştirilir. Özellikle SSD ve benzeri flash tabanlı depolama ortamlarında klasik üzerine yazma yöntemlerinin her durumda yeterli olmayabileceği dikkate alınır.

4.3.2. Fiziksel İmha

Elektronik ortamın yeniden kullanılmayacağı ve elden çıkarılacağı durumlarda, ortam üzerinde bulunan bilgilerin geri getirilemeyecek hale getirilmesi amacıyla uygun fiziksel imha yöntemi uygulanır.

İmha yöntemi ortamın türüne göre;

- Parçalama,
- Kırma,
- Delme,
- Ezme,
- Kesme,
- Yetkilendirilmiş elektronik atık imha hizmeti veya bilgi güvenliğini sağlayan eşdeğer yöntemlerden biri olabilir.

İmha yönteminin seçilmesinde ortamın türü ve üzerinde bulunan bilginin gizlilik/kritiklik seviyesi dikkate alınır.

4.4. Sunucu ve Veri Depolama Ortamlarının İmhası

1. Kullanım ömrü sona eren veya sistemden çıkarılan sunucu diskleri üzerinde bulunan veriler, sunucunun elden çıkarılmasından önce güvenli şekilde silinir veya fiziksel olarak imha edilir.
2. Gizli veya Çok Gizli bilgi, kişisel veri, özel nitelikli kişisel veri veya kritik sistem bilgisi içeren depolama ortamlarında güvenli silme veya fiziksel imha yöntemi tercih edilir.
3. Sunucu veya depolama ortamı üçüncü bir tarafa devredilecekse, devretme öncesinde üzerindeki verilerin güvenli şekilde silindiği doğrulanır.
4. Veri silme veya imha işlemleri mümkün olduğunda kayıt altına alınır.

4.5. Sanal Sunucu ve Sanal Disklerin İmhası

1. Kullanımdan kaldırılan sanal makineler ve sanal diskler üzerinde bulunan veriler, ilgili sanallaştırma altyapısının güvenli silme yöntemleri kullanılarak imha edilir.
2. Sanal makinenin silinmesi tek başına verilerin güvenli şekilde imha edildiği anlamına gelmediğinden, kullanılan sanallaştırma ve depolama altyapısına uygun güvenli silme işlemleri uygulanır.
3. Snapshot, yedek, replica ve benzeri kopyaların bulunması halinde bunların da ilgili saklama süresi ve imha kurallarına uygun şekilde değerlendirilmesi sağlanır.
4. Fiziksel depolama ortamının yeniden kullanılması veya elden çıkarılması söz konusu ise fiziksel depolama ortamı için ayrıca 4.3 Elektronik Ortamların İmhası hükümleri uygulanır.

4.6. Yedekleme Ortamlarının İmhası

1. Yedekleme ortamları, belirlenen saklama süresi sona ermeden imha edilmez.

2. Saklama süresi sona eren yedekleme ortamları, içerdiği bilgilerin niteliğine uygun güvenli silme veya fiziksel imha yöntemiyle imha edilir.
3. Yedekleme ortamlarında kişisel veri, özel nitelikli kişisel veri veya gizli bilgi bulunması halinde ilgili bilgi sınıflandırması ve kişisel veri saklama/imha kuralları dikkate alınır.
4. Yedekleme ortamlarının imha edilmesi, gerekli yedeklerin kaybedilmesine veya iş sürekliliğinin olumsuz etkilenmesine neden olmayacak şekilde planlanır.

4.7. Taşınabilir Cihazların İadesi ve İmhası

Laptop, tablet, mobil cihaz veya benzeri taşınabilir cihazlar;

- Kullanıcı değişikliği,
- Görevden ayrılma,
- Cihazın hurdaya ayrılması,
- Cihazın yenilenmesi,
- Cihazın başka bir kullanıcıya devredilmesi durumlarında bilgi güvenliği açısından kontrol edilir.

Cihaz yeniden kullanılacaksa üzerindeki kurumsal bilgiler güvenli şekilde silinir. Cihaz imha edilecekse depolama ortamının niteliğine uygun güvenli silme veya fiziksel imha yöntemi uygulanır.

4.8. Üçüncü Taraflara Teslim ve Elektronik Atık

1. Bilgi içeren elektronik ortamlar, yetkisiz üçüncü kişilere doğrudan teslim edilmez.
2. Elektronik atıkların kurum dışına çıkarılması gerektiğinde, bilgi içeren depolama ortamlarının güvenli şekilde silindiği veya fiziksel olarak imha edildiği doğrulanır.
3. Yetkilendirilmiş hizmet sağlayıcı kullanılması halinde, hizmet sağlayıcının güvenilirliği ve gerekli sözleşmesel yükümlülükleri değerlendirilir.
4. Gerektiğinde teslim ve imha işlemleri tutanak veya hizmet sağlayıcı tarafından verilen imha belgesi ile kayıt altına alınır.

4.9. Bilgi Sınıflandırmasına Göre İmha

İmha yöntemi bilgi varlığının sınıflandırması dikkate alınarak belirlenir.

Bilgi sınıfı	İmha yaklaşımı
Açık	Normal imha yöntemleri, ancak ortam yeniden kullanılacaksa veriler güvenli şekilde silinir.
Birime Özel	Yetkisiz kişilerin erişimini engelleyecek kontrollü imha yöntemi kullanılır.
Hizmete Özel	Kontrollü ve güvenli imha yöntemi uygulanır; gerektiğinde imha kaydı tutulur.

Gizli	Güvenli silme veya fiziksel imha uygulanır; imha işleminin kayıt altına alınması esastır.
Çok Gizli	Yetkili personel gözetiminde, geri getirilemeyecek şekilde güvenli silme veya fiziksel imha yapılır ve imha işlemi kayıt altına alınır.

Kişisel veri ve özel nitelikli kişisel veri içeren bilgi varlıklarında, bilgi sınıfından bağımsız olarak KVKK ve kişisel veri saklama/imha kuralları ayrıca dikkate alınır.

4.10. İmha Kayıtları

Gerektiğinde imha işlemi aşağıdaki bilgileri içerecek şekilde kayıt altına alınır:

- İmha tarihi,
- Birim,
- Bilgi varlığı/ortamın tanımı,
- Varlık veya cihaz numarası,
- Bilgi sınıfı,
- İmha nedeni,
- İmha yöntemi,
- İmha işlemini gerçekleştiren kişi/kişiler,
- Kontrol/onay bilgisi,
- Varsa imha tutanağı veya hizmet sağlayıcı belgesi.

Özellikle Gizli, Çok Gizli, kişisel veri veya özel nitelikli kişisel veri içeren ortamların imhasında kayıt tutulması esastır.

5. YAPTIRIM

Bu politikaya aykırı hareket edilmesi halinde olayın niteliğine göre;

- Olay Yönetimi Prosedürü,
- Kişisel Veri Yönetim Süreci,
- Düzeltici ve İyileştirici Faaliyet Prosedürü,
- Disiplin Prosedürü ve ilgili mevzuat hükümleri uygulanır.

Politikaya aykırı olarak bilgi içeren ortamın yetkisiz kişilere teslim edilmesi, kurum dışına çıkarılması veya güvenli olmayan yöntemlerle imha edilmesi bilgi güvenliği ve kişisel veri ihlali kapsamında ayrıca değerlendirilir.