1. AMAÇ

Bu prosedürün amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında bilgi varlıkları, kişisel veriler ve veri içeren fiziksel veya elektronik kayıt ortamlarının, ilgili mevzuat ve Üniversitenin saklama yükümlülükleri doğrultusunda saklama süresinin sona ermesi veya imha şartlarının oluşması durumunda güvenli ve kontrollü şekilde imha edilmesine ilişkin esasları belirlemektir.

Bu prosedür ile bilgi güvenliği, kişisel verilerin korunması ve veri gizliliğinin sağlanması; yetkisiz erişim, kullanım veya yeniden elde edilme risklerinin önlenmesi ve gerçekleştirilen imha işlemlerinin kayıt altına alınması amaçlanmaktadır.

2. KAPSAM

Bu prosedür; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi kapsamında gerçekleştirilen;

- Bilgi varlıklarını,
- Kişisel veri içeren kayıtları,
- Fiziksel ve elektronik kayıtları,
- Sunucu ve istemci sistemlerini,
- Sabit disk, SSD, USB bellek, hafıza kartı, optik disk, manyetik medya ve benzeri veri depolama ortamlarını,
- Bilişim cihazlarını,
- Veri tabanlarını,
- Sanal sunucuları ve sanal depolama alanlarını,
- Yedekleme ortamlarını,
- Kâğıt ve benzeri fiziksel kayıt ortamlarını,
- Saklama süresi sona eren veya imha edilmesi gereken diğer bilgi ve kayıtları kapsar.

3. SORUMLULAR

3.1. Yönetim Temsilcisi / EYS kapsamında yetkilendirilen sorumlular

- İmha faaliyetlerinin EYS kurallarına uygun şekilde yürütülmesini sağlamak,
- İmha uygulamalarının gerekli durumlarda izlenmesini ve değerlendirilmesini sağlamak.

3.2. Birim Yöneticileri

- Sorumlu oldukları bilgi ve kayıtların saklama sürelerinin takibini yapmak,
- İmha şartları oluşan kayıtları belirlemek,
- İmha işlemlerinin yetkili personel tarafından gerçekleştirilmesini sağlamak,
- Gerçekleştirilen imha işlemlerinin kayıt altına alınmasını sağlamak.

3.3. Bilgi İşlem Birimleri / Sistem Yöneticileri

- Elektronik ortamda bulunan veri ve bilgi varlıklarının güvenli şekilde silinmesi veya yok edilmesini sağlamak,
- Veri depolama ortamlarının imhasında uygun teknik yöntemin kullanılmasını sağlamak,

- İmha işlemlerinde bilgi güvenliği ve erişim kontrollerini uygulamak,
- Gerektiğinde imha işlemlerini kayıt altına almak ve ilgili birime bildirmek.

3.4. Tüm Personel

- Sorumluluğunda bulunan bilgi ve kayıtların yetkisiz şekilde silinmesini veya imha edilmesini önlemek,
- Saklama süresi sona eren veya imha edilmesi gereken kayıtları ilgili birime bildirmek,
- İmha işlemlerini bu prosedür ve ilgili EYS dokümanlarına uygun şekilde gerçekleştirmek.

4. TANIMLAR

- ***EYS:*** Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi.
- ***Kişisel Veri:*** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
- ***İmha:*** Saklama süresi sona eren veya işlenmesini gerektiren şartları ortadan kalkan verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi.
- ***Silme*****:** Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hâle getirilmesi işlemidir.
- ***Yok Etme:*** Kişisel verilerin hiç kimse tarafından erişilemez, geri getirilemez ve tekrar kullanılamaz hâle getirilmesi işlemidir.
- ***Anonim Hâle Getirme:*** Kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.
- ***İlgili Kişi:*** Kişisel verisi işlenen gerçek kişidir.
- ***Kişisel Veri Envanteri:*** Üniversitede gerçekleştirilen kişisel veri işleme faaliyetlerinin; veri kategorileri, işleme amaçları, veri konusu kişi grupları, aktarım bilgileri, saklama süreleri ve benzeri unsurlar bakımından kayıt altına alındığı envanterdir.
- ***Periyodik İmha:*** Kişisel verilerin işlenmesini gerektiren şartların tamamen ortadan kalkması hâlinde, belirlenen periyodik aralıklarla gerçekleştirilen silme, yok etme veya anonim hâle getirme işlemidir.

5. UYGULAMA

5.1. Varlıkların İmhası

Bilgi kayıt özelliğine sahip her türlü cihazın kullanım dışı bırakılması, elden çıkarılması, başka bir birime devredilmesi veya yeniden kullanıma sunulması öncesinde üzerinde bulunan bilgi ve veriler değerlendirilir.

Kişisel veri, gizli bilgi veya bilgi güvenliği açısından korunması gereken veriler içeren cihazlarda, cihazın tekrar kullanılmasından veya Üniversite dışına çıkarılmasından önce verilerin güvenli şekilde silinmesi veya gerekli durumlarda veri depolama ortamının fiziksel olarak imha edilmesi sağlanır.

Cihazın üzerinde bulunan verilerin yalnızca işletim sistemi üzerinden normal silme işlemiyle güvenli şekilde ortadan kaldırılamadığı durumlarda, kullanılan depolama teknolojisine uygun güvenli silme veya fiziksel imha yöntemi uygulanır. İmha işlemi sonrasında gerekli kontroller gerçekleştirilir ve işlem kayıt altına alınır

5.2. Verilerin Silinmesi Yöntemleri

Verilerin silinmesinde, verinin bulunduğu kayıt ortamının özelliklerine uygun yöntem kullanılır.

a) Kâğıt ortamındaki veriler:

Kâğıt ortamında bulunan kişisel veriler ve gizli bilgiler, kâğıt imha makinesi veya bilgilerin yeniden okunmasını ve bir araya getirilmesini engelleyecek uygun fiziksel imha yöntemi kullanılarak imha edilir. Kısmi karartmanın yeterli olmadığı durumlarda belgenin tamamının uygun şekilde imha edilmesi sağlanır.

b) Elektronik ortamda bulunan veriler:

Elektronik ortamda bulunan veriler, kullanılan sistemin ve depolama teknolojisinin özelliklerine uygun güvenli silme yöntemiyle silinir. Sadece işletim sisteminin normal silme komutunun kullanılması, verilerin yeniden elde edilmesi riski bulunan durumlarda tek başına yeterli kabul edilmez.

c) Veri tabanları:

Veri tabanlarında bulunan ve saklama süresi sona eren kişisel veriler, yetkili veri tabanı yöneticileri tarafından veri tabanı yapısının ve uygulamaların çalışmasını bozmayacak şekilde silinir. Silme işlemi sırasında veri bütünlüğü, ilişkili kayıtlar ve yasal saklama yükümlülükleri dikkate alınır.

d) Sanal sunucular ve sanal depolama alanları:

Sanal sunucunun veya sanal diskin silinmesi işlemi, kullanılan altyapının teknik özellikleri dikkate alınarak gerçekleştirilir. Sanal ortamın silinmesinin fiziksel depolama ortamındaki verileri güvenli şekilde ortadan kaldırmadığı durumlarda, altyapıya uygun ilave güvenli silme veya fiziksel imha yöntemi uygulanır.

e) Yedekleme ortamları:

İmha edilmesi gereken verilerin yedeklerde bulunması hâlinde yedekleme sisteminin saklama süreleri ve teknik yapısı dikkate alınır. Yedeklerin saklama süresi sona erdiğinde, yedekler kullanılan sistemin özelliklerine uygun şekilde güvenli olarak silinir veya fiziksel olarak imha edilir.

5.3. Varlıkların ve Verinin Yok Edilmesi Yöntemleri

Verilerin yok edilmesinde, verinin bulunduğu ortamın teknik özelliklerine ve bilgi sınıflandırma seviyesine uygun yöntem kullanılır.

a) Yerel sistemler ve veri depolama ortamları:

Sabit disk, SSD ve benzeri depolama ortamlarında; güvenli silme, uygun teknik yöntemlerle verilerin geri getirilemez hâle getirilmesi veya fiziksel yok etme yöntemlerinden uygun olanı kullanılır. Kullanılan yöntemin depolama teknolojisine uygun olması sağlanır.

b) Ağ ve güvenlik cihazları:

Switch, router, firewall ve benzeri ağ veya güvenlik cihazlarının kullanım dışı bırakılması durumunda cihaz üzerinde bulunan yapılandırma bilgileri, erişim bilgileri, kayıtlar ve varsa veri depolama ortamları güvenli şekilde silinir veya imha edilir.

c) Flash tabanlı ortamlar:

USB bellek, SSD, hafıza kartı ve benzeri flash tabanlı ortamlarda kullanılacak imha yöntemi, bu teknolojilerin özellikleri dikkate alınarak belirlenir. Gerekli durumlarda fiziksel imha yöntemi kullanılır.

d) Manyetik medya:

Manyetik bant ve benzeri manyetik ortamlarda, ortamın teknik özelliklerine uygun güvenli silme veya fiziksel imha yöntemi uygulanır.

e) SIM kart ve hafıza kartları:

SIM kart, hafıza kartı ve benzeri veri içerebilen ortamlar, üzerlerinde bulunan verilerin yeniden elde edilmesini önleyecek şekilde güvenli olarak silinir veya fiziksel olarak imha edilir.

f) Optik diskler:

CD, DVD ve benzeri optik diskler, üzerindeki verilerin yeniden okunmasını engelleyecek şekilde fiziksel olarak parçalanır veya uygun fiziksel imha yöntemi kullanılır.

g) Veri kayıt özelliği bulunan çevre birimleri:

Yazıcı, çok işlevli cihaz, kamera kayıt cihazı ve benzeri cihazlarda bulunan sabit veya taşınabilir veri depolama ortamları ayrıca değerlendirilir ve gerekli durumlarda güvenli şekilde silinir veya imha edilir.

h) Basılı ortamlar:

Kâğıt, çıktı, form, rapor ve benzeri fiziksel kayıtlar kâğıt imha makinesi veya uygun fiziksel imha yöntemiyle imha edilir.

5.4. İmha İlkeleri

İmha faaliyetleri aşağıdaki temel ilkeler doğrultusunda yürütülür.

5.4.1. Yasal ve Düzenleyici Uyum:

İmha işlemleri;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik,
- İlgili diğer mevzuat,
- Kurul kararları,
- Üniversitenin EYS dokümanları,
- Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası ile uyumlu olarak gerçekleştirilir.

Yasal, idari veya adli nedenlerle saklanması gereken kayıtlar, ilgili saklama yükümlülüğü sona ermeden imha edilmez.

5.4.2. İhtiyaca Dayalı İmha:

Bilgi ve kayıtlar, işlenme veya saklanma amacının gerektirdiği süreden daha uzun süre tutulmaz. Kişisel veriler bakımından saklama süreleri Kişisel Veri İşleme Envanteri, ilgili mevzuat ve Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası dikkate alınarak belirlenir.

5.4.3. Gizlilik ve Güvenlik:

İmha işlemi sırasında kişisel verilere ve gizli bilgilere yetkisiz kişilerin erişmesi engellenir. İmha işlemi gerçekleştirilecek kayıtlar, işlem tamamlanıncaya kadar güvenli alanlarda veya yetkili personelin kontrolünde muhafaza edilir.

5.4.4. Belirlenmiş İmha Süreçleri:

İmha işlemlerinde kullanılacak yöntem, verinin bulunduğu ortam ve veri niteliğine göre önceden belirlenir. İmha işlemi; uygun yöntemin seçilmesi, yetkilendirme, uygulama, kontrol ve kayıt aşamalarını kapsayacak şekilde gerçekleştirilir.

5.5. İmha Yöntemleri:

İmha yöntemleri, organizasyonların bilgi güvenliği standartlarına uygun olarak güvenli bir şekilde imha etmelerini sağlayan çeşitli yöntemleri içerir. İmha yöntemleri, kayıtların fiziksel veya dijital formatta olup olmadığına bağlı olarak farklılık gösterebilir.

5.5.1. Fiziksel Kayıtlar için İmha Yöntemleri:

- **Parçalama (Shredding):** Kâğıt ve benzeri fiziksel kayıtların okunamayacak ve yeniden oluşturulamayacak şekilde parçalanmasıdır.
- **Yakma (Incineration):** Belirli güvenlik standartlarına uygun olarak gerçekleştirilen yakma işlemi, kağıt belgelerin tamamen yok edilmesini sağlar. Ancak, çevresel etkileri nedeniyle dikkatlice ve uygun şekilde yapılmalıdır.
- **Öğütme (Pulping):** Kayıtların yeniden kullanılmasını veya okunmasını engelleyecek şekilde küçük parçalara ayrılmasıdır.
- **Fiziksel Yok Etme:** Veri depolama ortamlarının parçalanması, kırılması veya teknik olarak yeniden kullanılmasını ve verilerin elde edilmesini engelleyecek şekilde fiziksel olarak imha edilmesidir. Fiziksel imha yöntemi, kullanılan medya türünün özelliklerine uygun olarak gerçekleştirilir.

5.5.2. Dijital Kayıtlar için İmha Yöntemleri:

- **Güvenli Dijital Silme (Digital Erasure):** Verilerin kullanılan sistem veya depolama teknolojisine uygun yöntemlerle, yetkili kullanıcılar tarafından yeniden erişilemez hâle getirilmesidir.
- **Fiziksel Medya İmhası:** Verinin bulunduğu fiziksel depolama ortamının, verilerin yeniden elde edilmesini engelleyecek şekilde fiziksel olarak imha edilmesidir.
- **Fabrika Sıfırlama (Factory Reset):** Elektronik cihazlar, özellikle mobil cihazlar veya diğer veri depolama cihazları, fabrika sıfırlama işlemi ile bilgileri temizleyebilir. Ancak, bu işlem güvenli bir şekilde yapılmalıdır.
- **Manyetik Silme:** Manyetik bir ortamı kullanarak bilgileri silme işlemi, manyetik medyaların güvenli bir şekilde imha edilmesini sağlar.
- **Şifreleme Anahtarlarının İmhası:** Şifrelenmiş verilerin erişimini sağlayan anahtarların güvenli şekilde ortadan kaldırılması yoluyla verilere erişimin teknik olarak engellenmesidir. Bu yöntem yalnızca kullanılan şifreleme yapısının güvenlik gereksinimlerini karşılaması ve verilerin başka bir yöntemle erişilebilir olmaması durumunda uygun bir imha yöntemi olarak değerlendirilir.

- **Üzerine Yazma:** Uygun manyetik depolama ortamlarında, önceki verilerin yeniden elde edilmesini engelleyecek şekilde uygun teknik yöntemlerle üzerine veri yazılmasıdır.

5.6. Kişisel Verileri İmha Teknikleri

Kişisel verilerin işlenmesini gerektiren şartların tamamen ortadan kalkması hâlinde kişisel veriler; mevzuat, Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası ve bu prosedür doğrultusunda **silinir, yok edilir veya anonim hâle getirilir.** İmha yöntemi belirlenirken kişisel verinin bulunduğu kayıt ortamı, veri niteliği, bilgi güvenliği riski ve teknik imkânlar dikkate alınır.

5.6.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, ilgili kullanıcılar için verilerin hiçbir şekilde erişilemez ve tekrar kullanılamaz hâle getirilmesi şeklinde gerçekleştirilir.

Kişisel veriler Tablo-1'de verilen yöntemlerle silinir.

Tablo 1: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Yetkili sistem yöneticisi tarafından ilgili kullanıcıların erişimi kaldırılır ve veriler kullanılan sistemin teknik özelliklerine uygun güvenli yöntemle silinir.
Elektronik Ortamda Yer Alan Kişisel Veriler	Veriler, ilgili kullanıcılar tarafından erişilemez ve tekrar kullanılamaz hâle getirilir. Gerekli durumlarda erişim yetkileri kaldırılır ve güvenli silme uygulanır.
Veri tabanlarında yer alan kişisel veriler	Yetkili veri tabanı yöneticisi tarafından, uygulamanın veri bütünlüğü korunarak silme işlemi gerçekleştirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Belgeler, yetkisiz kişilerce okunamayacak ve tekrar kullanılamayacak şekilde fiziksel olarak imha edilir.
Taşınabilir Medyada Bulunan Kişisel Veriler	Kullanılan medya türüne uygun güvenli silme veya fiziksel imha yöntemi uygulanır.

5.6.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin hiç kimse tarafından erişilemez, geri getirilemez ve tekrar kullanılamaz hâle getirilmesinin gerektiği durumlarda yok etme yöntemi uygulanır.

Tablo 2: Kişisel Verilerin Yok edilmesi

Kâğıt ortamı	Kâğıtların parçalanması veya uygun fiziksel imha yöntemi
Optik medya	Parçalama veya uygun fiziksel imha yöntemi
Manyetik medya	Ortamın özelliklerine uygun güvenli silme veya fiziksel imha
Sabit disk / SSD	Güvenli silme veya uygun fiziksel imha
USB / hafıza kartı	Güvenli silme veya fiziksel imha
Diğer veri depolama ortamları	Ortamın teknik özelliklerine uygun güvenli silme veya fiziksel imha

5.6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hâle getirilmesi, verilerin başka verilerle eşleştirilmesi durumunda dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi suretiyle gerçekleştirilir. Anonimleştirme işlemi yapılırken verilerin tekrar kişisel veri niteliği kazanmasına neden olabilecek eşleştirme ve geri döndürme ihtimalleri dikkate alınır. Anonimleştirme işlemi sonrasında verilerin anonimlik niteliği gerekli durumlarda kontrol edilir.

5.7. Veri Türlerine Göre Saklanma Ve İmha Süreleri

Kişisel veri ve diğer kayıtların saklama süreleri belirlenirken ilgili mevzuat, Üniversitenin idari ve hukuki yükümlülükleri, Kişisel Veri İşleme Envanteri ve Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası esas alınır. Saklama süresi dolan kişisel veriler, imha yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde silinir, yok edilir veya anonim hâle getirilir. Periyodik imha aralığı Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası ile belirlenir ve mevzuatta öngörülen sürelere uygun olarak yürütülür.

Tablo 3 : Kişisel Veri Saklama ve İmha Süreleri

Veri / Kayıt Türü	**Muhafaza Süresi**	**İmha Süresi**
Personel özlük ve personel kayıtları	İlgili mevzuat, Üniversite düzenlemeleri ve Kişisel Veri Envanteri	Saklama süresinin sona ermesini takip eden ilk periyodik imha
Öğrenci kayıtları	İlgili mevzuat, Üniversite düzenlemeleri ve Kişisel Veri Envanteri	Saklama süresinin sona ermesini takip eden ilk periyodik imha

Personel adaylarına ilişkin kayıtlar	İlgili mevzuat ve Kişisel Veri Envanteri	Saklama süresinin sona ermesini takip eden ilk periyodik imha
Kamera kayıtları	İlgili mevzuat, güvenlik ihtiyaçları ve Üniversite düzenlemeleri	Saklama süresinin sona ermesini takip eden ilk periyodik imha
Sistem ve uygulama log kayıtları	Bilgi güvenliği, mevzuat ve ilgili EYS dokümanları	Belirlenen saklama süresinin sona ermesini takip eden ilk uygun imha
Elektronik posta kayıtları	İlgili mevzuat, bilgi güvenliği ve Üniversite düzenlemeleri	Saklama süresinin sona ermesini takip eden ilk uygun imha
Resmî yazışmalar ve arşiv kayıtları	İlgili mevzuat ve arşiv düzenlemeleri	İlgili saklama/arşiv süresi sonunda
Sözleşme ve satın alma kayıtları	İlgili mevzuat ve Üniversite düzenlemeleri	Saklama süresinin sona ermesini takip eden ilk uygun imha
Mali ve muhasebe kayıtları	İlgili mali mevzuat ve Üniversite düzenlemeleri	Yasal saklama süresinin sona ermesini takip eden ilk uygun imha
Yedekleme kayıtları	Bilgi güvenliği ve yedekleme süreçlerinde belirlenen süreler	Yedekleme yaşam döngüsünün sonunda uygun yöntemle imha

Tabloda belirtilen kayıt türlerinin saklama süreleri, ilgili mevzuat veya Üniversitenin yürürlükteki düzenlemeleri doğrultusunda güncellenir. Mevzuatta farklı bir süre öngörülmesi hâlinde mevzuat hükümleri esas alınır.

5.8. İlgili Kişinin Talebi Üzerine İmha

İlgili kişinin kişisel verilerinin silinmesi veya yok edilmesine yönelik başvurusu, ilgili kişi başvurularının yönetilmesine ilişkin süreç kapsamında değerlendirilir.

Kişisel verilerin işlenmesini gerektiren şartların tamamen ortadan kalkmış olması hâlinde talebe konu veriler mevzuatta öngörülen süre içerisinde silinir, yok edilir veya anonim hâle getirilir. Kişisel verilerin işlenmesini gerektiren şartların devam etmesi hâlinde talep, gerekçesi belirtilerek ilgili mevzuat kapsamında değerlendirilir. Kişisel verilerin üçüncü kişilere aktarılmış olması ve imha şartlarının oluşması durumunda gerekli bildirim ve işlemler ilgili mevzuata uygun olarak gerçekleştirilir.

5.9. İmha İşlemlerinin Kayıt Altına Alınması

Gerçekleştirilen kişisel veri imha işlemleri kayıt altına alınır. İmha kayıtlarında mümkün olduğu ölçüde;

- İmha tarihi,
- İmha edilen veri veya kayıt türü,
- İmha edilen kayıt ortamı,
- İmha yöntemi,
- İmha kapsamı,
- İmha işlemini gerçekleştiren birim veya personel,
- Gerekli durumlarda imha işlemini kontrol eden kişi bilgilerine yer verilir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin işlemler kayıt altına alınır ve bu kayıtlar ilgili mevzuatta belirtilen süre boyunca muhafaza edilir.

5.10. İmha İşlemlerinin Kontrolü

İmha işlemi tamamlandıktan sonra gerekli durumlarda işlemin amacına uygun şekilde gerçekleştirildiği kontrol edilir. Elektronik ortamdaki imhalarda;

- İlgili veriye erişilemediği,
- Yetkili olmayan kullanıcıların veriye erişemediği,
- Verinin yeniden kullanılabilir durumda olmadığı,
- İmha edilen verinin başka bir aktif ortamda bulunup bulunmadığı kontrol edilir.

Fiziksel imhalarda ise imha edilen kayıt veya medya üzerinde bulunan bilgilerin okunabilir veya yeniden kullanılabilir durumda olmadığı kontrol edilir. Tespit edilen uygunsuzluklar ilgili birim yöneticisine bildirilir ve gerekli düzeltici işlemler gerçekleştirilir.

5.11. Üçüncü Taraflar Tarafından Gerçekleştirilen İmha İşlemleri

Üçüncü taraf hizmet sağlayıcılar tarafından gerçekleştirilecek imha işlemleri, Üniversitenin bilgi güvenliği ve kişisel verilerin korunmasına ilişkin kurallarına uygun olarak gerçekleştirilir. Üçüncü taraflara imha amacıyla teslim edilen veri veya kayıtların kapsamı, imha yöntemi ve işlem sonucu gerekli durumlarda kayıt altına alınır. Gerekli görülmesi hâlinde üçüncü taraftan imha işleminin gerçekleştirildiğini gösteren kayıt veya rapor alınır.

5.12. İmha Edilecek Varlıkların Geçici Olarak Muhafazası

İmha işlemi gerçekleştirilinceye kadar imha edilmesi gereken bilgi, belge ve veri depolama ortamları yetkisiz erişime karşı korunur. İmha edilecek fiziksel ortamların açıkta bırakılmaması, yetkisiz kişilere teslim edilmemesi ve imha işlemi tamamlanıncaya kadar ilgili birimin kontrolünde tutulması sağlanır.

6. İLGİLİ DOKÜMANLAR

- Taşınır Kayıt Prosedürü
- İmha Edilen Kayıt Listesi
- Medya İmha Raporu
- 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat
- Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası
- Kişisel Veri Envanter Listesi

7. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	23.08.2023	İlk yayın.
001	10.02.2025	Kişisel veri imha yöntemi eklenerek imha yöntemleri uygulamaları genişletilmiştir.
002	16.09.2026	Prosedürün Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi yapısına uyarlanması; kapsam, sorumluluklar, tanımlar, imha yöntemleri, kişisel veri imha süreçleri, saklama ve imha süreleri, kayıt ve kontrol faaliyetlerinin güncellenmesi.