1. AMAÇ

Bu prosedürün amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında kullanılan bilgi varlıkları, bilişim cihazları, veri depolama ortamları ve bunları destekleyen fiziksel altyapının güvenli şekilde kullanılması, taşınması, yer değiştirilmesi, bakım ve onarımının yapılması, kullanım dışı bırakılması ve elden çıkarılması sırasında uygulanacak esasları belirlemektir.

Bu prosedür ile cihaz ve medya üzerinde bulunan bilgi ve kişisel verilerin yetkisiz erişim, kayıp, ifşa, bozulma veya geri döndürülebilir şekilde silinme risklerinin azaltılması; bilgi güvenliği, kişisel verilerin korunması, iş sürekliliği, bilişim hizmetlerinin sürekliliği ve kalite gerekliliklerinin desteklenmesi amaçlanmaktadır.

2. KAPSAM

Bu prosedür; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilinde kullanılan veya EYS kapsamında kontrol edilen;

- masaüstü ve dizüstü bilgisayarlar,
- sunucular ve veri depolama sistemleri,
- sabit diskler ve SSD'ler,
- harici diskler,
- USB bellekler,
- CD/DVD ve benzeri optik medya,
- hafıza kartları,
- taşınabilir bilgisayar, tablet ve benzeri cihazlar,
- yazıcı, tarayıcı ve çok işlevli cihazların veri depolama birimleri,
- ağ ve iletişim cihazları,
- veri ve enerji kabloları,
- diğer bilgi taşıyan veya bilgi hizmetlerini destekleyen cihaz ve medya

ile bunların güvenli silinmesi, imhası, taşınması, yer değiştirilmesi, bakım ve onarımı faaliyetlerini kapsar.

3. SORUMLULUK

Bu prosedürün uygulanmasından;

- **Üst Yönetim**, gerekli kaynakların ve organizasyonel şartların sağlanmasından,
- **İlgili Birim Yöneticileri**, kendi sorumluluk alanlarındaki cihaz ve medya kontrollerinin yürütülmesinden,
- **EYS kapsamında ilgili süreç ve varlık sorumluları**, cihaz ve medya üzerinde bulunan bilgi varlıklarının uygun şekilde korunmasından,

- **Bilgi İşlem / teknik birimler**, bilişim cihazlarının teknik bakım, onarım, güvenli silme, imha ve gerekli kontrollerinin gerçekleştirilmesinden,
- **Cihazı kullanan veya zimmetinde bulunduran personel**, cihaz ve medyanın korunması, yetkisiz kişilere teslim edilmemesi ve prosedüre uygun hareket edilmesinden,
- **Tüm çalışanlar**, kendilerine teslim edilen cihaz ve medyanın güvenli kullanımından ve tespit edilen kayıp, hasar, arıza veya güvenlik olaylarını ilgili birime bildirmekten sorumludur.

4. UYGULAMA

4.1. Cihaz ve Medya Kullanımına İlişkin Genel Esaslar

- Kurum tarafından kullanılan cihaz ve medya, yalnızca yetkilendirilmiş amaçlar doğrultusunda ve ilgili bilgi güvenliği, kişisel veri, iş sürekliliği ve bilişim hizmetleri kurallarına uygun olarak kullanılır.
- Bilgi içeren cihaz ve medyanın yetkisiz kişiler tarafından kullanılmasına, erişilmesine, taşınmasına veya kurum dışına çıkarılmasına izin verilmez.
- Bilgi içeren cihazların elden çıkarılması, başka bir kullanıcıya devredilmesi, birimler arasında yer değiştirmesi veya kurum dışına çıkarılması öncesinde cihaz üzerindeki bilgilerin korunması ve gerekli ise güvenli şekilde silinmesi sağlanır.
- Cihaz veya medya üzerinde kişisel veri, gizli bilgi, kurumsal bilgi veya diğer koruma gerektiren bilgiler bulunması halinde ilgili bilgi sınıfına uygun güvenlik tedbirleri uygulanır.
- Kullanım dışı bırakılan cihaz ve medyanın üzerinde bulunan bilgilerin yeniden erişilebilir hale getirilmesini önleyecek yöntemler uygulanır.

4.2. Veri Silme ve Medya İmhası Önce Kontroller

4.2.1. Masaüstü ve Dizüstü Bilgisayarlar

a) Bir bilgisayarın kullanım dışı bırakılması, başka bir kullanıcıya devredilmesi, kurum dışına çıkarılması veya elden çıkarılması öncesinde üzerinde kurumsal bilgi veya kişisel veri bulunup bulunmadığı kontrol edilir.
b) Cihaz üzerinde bulunan ve saklanması gereken bilgiler, yetkilendirilmiş kurumsal ortama aktarılır.
c) Saklanmasına gerek bulunmayan bilgiler, uygun ve güvenli veri silme yöntemi kullanılarak silinir.
ç) Veri silme işleminin gerçekleştirilemediği veya depolama ortamının teknik olarak güvenli şekilde silinemediği durumlarda ilgili medya fiziksel imha sürecine alınır.
d) Kullanım dışı bırakılan cihazların kurum dışına çıkarılması veya üçüncü kişilere teslim edilmesi öncesinde veri içeren depolama ortamlarının güvenli şekilde temizlendiği kontrol edilir.
e) Veri silme veya medya imha işlemleri yetkili personel tarafından gerçekleştirilir ve gerekli işlemler kayıt altına alınır.

4.2.2. Sabit Disk, SSD ve Harici Depolama Birimleri

a) Kullanım dışı bırakılan veya başka bir kullanıcıya devredilecek sabit disk, SSD, harici disk ve benzeri depolama ortamları üzerindeki bilgiler güvenli şekilde silinir.
b) Teknik nedenlerle güvenli silme yapılamayan depolama ortamları fiziksel imha işlemine tabi tutulur.
c) İmha edilen medya için ilgili medya imha kaydı/raporu düzenlenir.
ç) İmha işlemi tamamlanmadan bilgi içeren medya atık, hurda veya benzeri toplama alanlarına bırakılmaz.

4.2.3. CD/DVD ve Optik Medya

a) Kurumsal bilgi içeren CD/DVD ve benzeri optik medyalar kullanım dışı bırakılmadan önce üzerlerindeki bilgilerin yetkisiz şekilde elde edilmesini engelleyecek yöntemlerle imha edilir.
b) İmha edilecek medya, içeriğine uygun şekilde fiziksel olarak kullanılamaz hale getirilir.
c) Gerekli durumlarda imha işlemi kayıt altına alınır.

4.2.4. USB Bellek ve Hafıza Kartları

a) USB bellek, hafıza kartı ve benzeri taşınabilir depolama ortamlarında bulunan kurumsal bilgiler yetkisiz kişilerin erişimine karşı korunur.
b) Kullanım dışı bırakılacak medya üzerinde bulunan ve saklanması gereken bilgiler yetkilendirilmiş ortama aktarılır.
c) Saklanmasına gerek olmayan bilgiler güvenli veri silme yöntemi ile silinir.
ç) Silme veya biçimlendirme işleminin güvenli şekilde gerçekleştirilemediği durumlarda medya fiziksel olarak imha edilir.
d) Kayıp, çalınma veya yetkisiz erişim şüphesi bulunan taşınabilir medya, ilgili bilgi güvenliği/olay yönetimi süreci kapsamında değerlendirilir.

4.3. Cihaz ve Medyanın Yer Değiştirmesi ve Taşınması

4.3.1. Genel Esaslar

a) Bilgi içeren cihaz ve medyanın birim içerisinde veya birimler arasında taşınması sırasında yetkisiz erişim, kayıp, hasar ve bilgi ifşasına karşı gerekli tedbirler alınır.
b) Cihaz veya medya, taşıma sırasında yetkisiz kişilerin erişimine açık bırakılmaz.
c) Kritik veya hassas bilgi içeren cihazların taşınması gerektiğinde, taşıma işlemi yetkilendirilmiş personel tarafından gerçekleştirilir.
ç) Üçüncü kişilerden taşıma hizmeti alınması halinde cihaz ve medya üzerindeki bilgilerin güvenliği için gerekli kontrol ve tedbirler uygulanır.
d) Cihazın teslimi ve devri gerektiğinde zimmet, teslim-tesellüm veya ilgili kayıt mekanizmaları kullanılır.

4.3.2. Masaüstü ve Dizüstü Bilgisayarlar

a) Cihazların yer değiştirmesi sırasında cihazın fiziksel bütünlüğü korunur.
b) Kurum dışına çıkarılması gereken cihazlarda ilgili yetkilendirme ve teslim kayıtları oluşturulur.

c) Cihazın üçüncü kişilere teslim edilmesi gerektiğinde, mümkün olan durumlarda cihaz üzerindeki bilgi ve verilerin korunmasına yönelik gerekli tedbirler alınır.

4.3.3. Taşınabilir Medya

USB bellek, harici disk, hafıza kartı ve benzeri taşınabilir medyanın taşınması sırasında;

- kayıp ve çalınmaya,
- yetkisiz erişime,
- fiziksel hasara,
- yetkisiz kişilere teslim edilmeye karşı gerekli tedbirler alınır.

4.4. Cihazların Kurum Dışına Çıkarılması

a) Kuruma ait cihazların kurum dışına çıkarılması, ilgili yetkilendirme ve teslim süreçlerine uygun olarak gerçekleştirilir.
b) Kurum dışına çıkarılan cihazlarda bulunan bilgiler, bilgi sınıflandırma ve ilgili güvenlik kurallarına uygun şekilde korunur.
c) Kurum dışına çıkarılan taşınabilir cihazların kaybolması, çalınması veya yetkisiz erişime maruz kalması halinde durum derhal ilgili birime bildirilir.
ç) Kurum dışına çıkarılması planlanan ve kullanım dışı bırakılacak cihazların depolama ortamlarında bulunan bilgiler, cihazın dışarı çıkarılmasından önce güvenli şekilde silinir veya medya imha sürecine alınır.

4.5. Kablolama ve Fiziksel Bağlantılar

a) Veri taşıyan veya bilgi hizmetlerini destekleyen elektrik, haberleşme ve ağ kabloları; kesilme, ezilme, kopma, fiziksel hasar ve yetkisiz müdahaleye karşı korunacak şekilde yerleştirilir.
b) Veri ve enerji kablolarının mümkün olduğunca uygun kanallar ve koruyucu sistemler içerisinde düzenli şekilde tesis edilmesi sağlanır.
c) Kablolar; kopma, ezilme, aşırı ısınma, nem, korozyon, elektromanyetik etkiler ve benzeri fiziksel koşullara karşı uygun şekilde korunur.
ç) Kablo ve bağlantılarda arıza, hasar, aşınma veya kesinti tespit edilmesi halinde ilgili teknik birime bildirim yapılır.
d) Yapılan bakım, onarım veya değişiklikler ilgili kayıtlarla izlenebilir hale getirilir.

4.6. Sistem, Cihaz Ve Medya Bakım Ve Onarımı

a) Kurum bünyesinde kullanılan bilişim cihazları, medya sistemleri ve ilgili teknik altyapının bakım ve kontrolleri, belirlenen bakım planları doğrultusunda gerçekleştirilir.
b) Bakım ve onarım faaliyetleri yetkilendirilmiş teknik personel veya uygun şekilde yetkilendirilmiş hizmet sağlayıcılar tarafından gerçekleştirilir.
c) Bakım veya onarım amacıyla cihazın kurum dışına gönderilmesi gerektiğinde, cihaz üzerinde bulunan bilgilerin güvenliği değerlendirilir ve gerekli koruma tedbirleri alınır.

ç) Cihazın bakım veya onarım için üçüncü kişilere teslim edilmesi durumunda, bilgi güvenliği ve kişisel verilerin korunmasına yönelik gerekli kontroller uygulanır.
d) Bakım ve onarım faaliyetleri sonrasında yapılan işlem, kullanılan parça/ekipman ve cihazın durumu ilgili bakım ve onarım kayıtlarıyla izlenebilir hale getirilir.
e) Normal çalışma koşullarını yerine getirmeyen cihazlar teknik değerlendirme sonucuna göre onarılır, güncellenir, değiştirilir veya kullanım dışı bırakılır.
f) Bakım ve onarım sırasında bilgi güvenliği, kişisel verilerin korunması ve iş sürekliliği açısından gerekli tedbirler alınır.

4.7. Kullanım Dışı Bırakma ve İmha

a) Kullanım dışı bırakılan cihaz ve medyanın üzerinde bilgi bulunup bulunmadığı belirlenir.
b) Saklanması gereken bilgiler yetkilendirilmiş ortamlara aktarılır.
c) Bilgi içeren medya, güvenli silme veya fiziksel imha yöntemlerinden uygun olanı kullanılarak kullanılamaz hale getirilir.
ç) Fiziksel imha gerektiren medya, imha işlemi gerçekleştirilinceye kadar yetkisiz erişime karşı güvenli bir alanda muhafaza edilir.
d) Medya imha işlemi tamamlandığında ilgili imha kaydı/raporu oluşturulur.
e) İmha edilen medya ve cihazların kayıtları, ilgili EYS kayıt saklama kurallarına uygun şekilde muhafaza edilir.

5. İLGİLİ DOKÜMANLAR

- Bakım ve Onarım Raporu
- Medya İmha Raporu
- Veri Merkezleri ve Elektrik Odası Günlük Fiziki Kontrol Tutanağı
- Sunucular Günlük Fiziki Kontrol Tutanağı
- Sunucu Günlük Kontrol planı

6. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	22.01.2020	İlk yayın.
001	27.09.2022	İlgili Dokümanlar kısmı güncellenmiştir.
002	22.01.2024	Kontrol kısmı güncellenmiştir.
003	16.09.2026	Doküman, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi yapısına uygun olarak kapsam, sorumluluklar, cihaz ve medya yönetimi, güvenli veri silme, medya imhası, taşıma ve yer değiştirme, kurum dışına çıkarma, kablolama, bakım ve onarım, kullanım dışı bırakma ve kayıtların yönetimi açısından yeniden düzenlenmiştir.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü – Zekai KÜNAR	Doç. Dr. - Mevlüt ERSOY