1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında kullanılan bilgi teknolojileri teçhizatının kullanım ömrünün sona ermesi, arızalanması, teknolojik olarak yetersiz kalması veya başka bir nedenle kullanım dışı bırakılması ve elden çıkarılması sırasında bilgi güvenliği, kişisel verilerin korunması ve varlık kayıtlarının izlenebilirliğinin sağlanmasıdır.

2. KAPSAM

Bu politika; Süleyman Demirel Üniversitesi Daire Başkanlıklar, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi kapsamında kullanılan veya yönetilen;

- Sunucu ve bilgisayarları,
- Dizüstü bilgisayar ve diğer uç cihazları,
- Ağ ve iletişim cihazlarını,
- Bilgi depolama özelliğine sahip teçhizatı,
- Sabit disk, SSD, USB bellek, hafıza kartı ve benzeri depolama ortamlarını ve bunların yeniden kullanıma hazırlanması, veri silme, imha ve elden çıkarma süreçlerini kapsar.

3. SORUMLULUKLAR

3.1. Bilgi İşlem Daire Başkanlığı

- Elden çıkarılacak bilgi teknolojileri teçhizatının bilgi güvenliği kurallarına uygun şekilde işleme alınmasını sağlamak,
- Teçhizat üzerindeki bilgi depolama ortamlarını belirlemek,
- Gerekli veri silme veya fiziksel imha işlemlerinin gerçekleştirilmesini sağlamak,
- Elden çıkarma ve imha işlemlerine ilişkin kayıtların tutulmasını sağlamak,
- İlgili varlık ve sistem envanterlerinin güncellenmesini sağlamak.

3.2. Birim Yöneticileri

- Kullanım dışı bırakılması gereken teçhizatı ilgili birimlere bildirmek,
- Teçhizatın yetkisiz kişilere teslim edilmesini önlemek,
- Gerekli devir ve elden çıkarma kayıtlarının oluşturulmasını sağlamak.

3.3. Teçhizat Kullanıcıları

- Kullanımındaki teçhizatın arızalanması veya kullanım dışı kalması durumunu ilgili birime bildirmek,
- Teçhizat elden çıkarılıncaya kadar üzerindeki bilgi ve verilerin güvenliğini korumak,
- Teçhizatı yetkisiz kişilere teslim etmemek.

4. UYGULAMA

4.1. Kullanım Dışı Bırakma

1. Kullanım ömrünü tamamlayan, ekonomik veya teknik açıdan kullanılması uygun olmayan, arızalı veya başka bir nedenle kullanım dışı bırakılan teçhizat belirlenir.
2. Elden çıkarma işleminden önce teçhizatın yeniden kullanılıp kullanılamayacağı değerlendirilir.
3. Yeniden kullanılacak teçhizat ile tamamen elden çıkarılacak teçhizat birbirinden ayrılır.

4.2. Yeniden Kullanım

1. Yeniden kullanılmasına karar verilen teçhizat üzerinde önceki kullanıcıya veya sisteme ait hesap, parola, sertifika, kriptografik anahtar, yapılandırma ve benzeri erişim bilgilerinin bırakılmaması sağlanır.
2. Teçhizat üzerindeki veriler, ilgili bilgi sınıflandırması ve risk düzeyi dikkate alınarak güvenli şekilde silinir.
3. Teçhizat yeniden kullanım öncesinde gerekli güvenlik yapılandırmaları yapılarak ilgili kullanıcı veya birime tahsis edilir.

4.3. Sunucu ve Bilgisayarlar

1. Elden çıkarılacak sunucu, bilgisayar ve benzeri cihazlarda bulunan veri depolama ortamları belirlenir.
2. Bu ortamlarda bulunan veriler, teçhizat kurum dışına çıkarılmadan veya üçüncü taraflara teslim edilmeden önce güvenli şekilde silinir veya uygun yöntemle fiziksel olarak imha edilir.
3. Veri içeren depolama ortamlarının yalnızca cihazdan sökülmesi, veri imhası olarak kabul edilmez. Verilerin güvenli şekilde silindiği veya ortamın fiziksel olarak imha edildiği kayıt altına alınır.
4. Elden çıkarma işlemi tamamlanan teçhizat ilgili varlık ve sistem envanterlerinden düşülür.

4.4. Ağ Cihazları

1. Elden çıkarılacak yönlendirici, anahtar, güvenlik duvarı, kablosuz ağ cihazı ve benzeri ağ cihazlarının yapılandırmaları güvenli şekilde kaldırılır.
2. Cihazlarda bulunan;

- IP adresleri,
- Kullanıcı adı ve parolalar,
- Erişim bilgileri,
- Sertifikalar,
- Kriptografik anahtarlar,

- Diğer güvenlik açısından hassas yapılandırma bilgileri silinir veya güvenli şekilde kaldırılır.

3. Cihaz, uygun güvenli sıfırlama yöntemi kullanılarak elden çıkarılmaya hazır hale getirilir.
4. Elden çıkarılan ağ cihazları sistem ve varlık envanterlerinden düşülür.

4.5. Veri Depolama Ortamlarının İmhası

1. Veri depolama ortamlarının imha yöntemi; ortamın türü, üzerinde bulunan bilginin sınıflandırması ve risk seviyesi dikkate alınarak belirlenir.
2. Gerektiğinde güvenli veri silme, üzerine yazma, fiziksel parçalama veya başka uygun imha yöntemleri kullanılır.
3. Kişisel veri içeren depolama ortamlarının imhası Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası doğrultusunda gerçekleştirilir.
4. Taşınabilir depolama ortamlarının imhasında Taşınabilir Ortamın İmhası Politikası hükümleri uygulanır.
5. İmha edilen depolama ortamları için ilgili imha kayıtları oluşturulur.

4.6. Elden Çıkarma ve Envanterden Düşme

1. Veri güvenliği kontrolleri tamamlanmadan bilgi teknolojileri teçhizatı kurum dışına çıkarılamaz veya üçüncü taraflara teslim edilemez.
2. Elden çıkarma işlemi tamamlanan teçhizatın varlık envanterindeki durumu güncellenir.
3. Elden çıkarma işleminin izlenebilirliğini sağlamak amacıyla teçhizatın tanımlayıcı bilgileri, işlem tarihi, gerçekleştirilen işlem ve gerekli durumlarda işlemi gerçekleştiren kişi/birim kayıt altına alınır.

4.7. Kayıp, Çalınma veya Yetkisiz Elden Çıkarma

Teçhizatın kaybolması, çalınması veya yetkisiz şekilde elden çıkarıldığının tespit edilmesi halinde durum Olay İhlal Prosedürü kapsamında değerlendirilir.

Kişisel veri veya bilgi güvenliği ihlali şüphesi bulunması halinde ilgili değerlendirme, bildirim ve kayıt süreçleri uygulanır.

5. YAPTIRIM

Bu politikaya aykırı uygulamalar EYS kapsamında uygunsuzluk olarak değerlendirilir ve gerekli durumlarda Düzeltici Faaliyet Prosedürü kapsamında işlem başlatılır. Çalışanların politika hükümlerine aykırı hareket etmesi halinde ilgili mevzuat, Üniversite düzenlemeleri ve Disiplin Prosedürü hükümleri uygulanır.