1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında yer alan bilgi, yazılım, donanım, bilgi teknolojileri, hizmet ve diğer kurumsal varlıkların belirlenmesi, sahiplerinin atanması, sınıflandırılması, korunması, kullanılması, izlenmesi ve yaşam döngüleri boyunca uygun şekilde yönetilmesine ilişkin esasları belirlemektir.

2. KAPSAM

Bu politika, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında yer alan;

- Daire Başkanlıklarını,
- Genel Sekreterliği,
- Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimini,
- bu birimlerde görev yapan çalışanları,
- Üniversite bilgi varlıklarını kullanan yetkili kullanıcıları,
- görev ve faaliyetleri kapsamında Üniversite varlıklarına erişen ilgili üçüncü tarafları kapsar.

Politika; bilgi varlıkları, bilgi teknolojileri varlıkları, donanım, yazılım, bilgi sistemleri, ağ ve iletişim altyapıları, elektronik ve fiziksel bilgi ortamları ile bunlarla ilişkili diğer varlıkları kapsar.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından;

- EYS kapsamındaki birim yöneticileri,
- varlık sahipleri,
- Bilgi İşlem Daire Başkanlığı ve ilgili bilgi işlem birimleri,
- bilgi varlıklarını kullanan tüm yetkili kullanıcılar sorumludur.

3.1. Birim Yöneticilerinin Sorumlulukları

- Birimleri bünyesindeki varlıkların belirlenmesini,
- Varlıkların envantere dahil edilmesini,
- Varlık sahiplerinin belirlenmesini,
- Varlıkların uygun şekilde korunmasını,

- Varlık bilgilerinin güncel tutulmasını sağlar.

3.2. Varlık Sahiplerinin Sorumlulukları

- Sorumluluklarındaki varlıkların doğru şekilde tanımlanmasını,
- Varlıkların uygun şekilde sınıflandırılmasını,
- Varlıkların kullanım ve erişim kurallarının belirlenmesini,
- Varlıkların güvenlik gereksinimlerinin belirlenmesini,
- Varlık bilgilerinin güncel tutulmasını sağlar.

3.3. Bilgi İşlem Birimlerinin Sorumlulukları

Bilgi İşlem Daire Başkanlığı ve ilgili bilgi işlem birimleri, sorumluluk alanlarındaki bilgi sistemleri ve teknolojik varlıkların teknik yönetimini, kullanıcı erişim yetkilerinin yönetimini ve gerekli teknik güvenlik kontrollerinin uygulanmasını sağlar.

4. UYGULAMA

4.1. Varlık Envanteri

- EYS kapsamındaki bilgi ve bilgi teknolojileri varlıkları, ilgili birimler bazında oluşturulan varlık envanterlerinde kayıt altına alınır.
- Varlık envanterinde varlığın adı, türü, bulunduğu birim, varlık sahibi, sorumlusu, sınıflandırması ve ihtiyaç duyulan diğer bilgiler tanımlanır.
- Yeni edinilen, geliştirilen veya hizmete alınan varlıklar uygun şekilde envantere dahil edilir.
- Kurum bünyesinde geliştirilen sistem ve yazılımlar da varlık envanterine dahil edilir.
- Varlık envanterleri en az yılda bir kez ve önemli değişiklikler meydana geldiğinde gözden geçirilerek güncellenir.
- Kullanımdan kaldırılan, devredilen, kaybolan veya imha edilen varlıkların envanter kayıtları güncellenir.

4.2. Varlık Sahipliği ve Sınıflandırma

- Yeni oluşturulan veya edinilen bilgi varlıkları için uygun bir varlık sahibi belirlenir.
- Bilgi varlıkları, gizlilik, bütünlük ve erişilebilirlik gereksinimleri dikkate alınarak kurumun bilgi sınıflandırma kurallarına uygun şekilde sınıflandırılır.
- Kişisel veri ve özel nitelikli kişisel veri içeren varlıklar, ilgili mevzuat ve EYS kapsamında belirlenen kişisel veri güvenliği kurallarına uygun şekilde korunur.

- Varlık sahipleri, sorumluluklarındaki varlıkların uygun kullanım ve korunma koşullarını belirler.

4.3. Kullanıcı Erişimleri ve Ayrıcalıkların Yönetimi

- Bilgi sistemlerine erişim yalnızca görev ve sorumlulukları doğrultusunda yetkilendirilmiş kullanıcılara sağlanır.
- Kullanıcı erişim yetkileri görev, birim veya sorumluluk değişikliklerinde gözden geçirilir ve gerekli güncellemeler yapılır.
- Kullanıcı ayrıcalıkları belirlenen periyotlarda gözden geçirilir.
- Ayrıcalıklı kullanıcı hesaplarının kullanımı kontrollü şekilde gerçekleştirilir.
- Bilgi sistemlerinde gerçekleştirilen erişim ve güvenlik açısından gerekli işlemler, ilgili mevzuat ve EYS dokümanlarında belirlenen kurallar doğrultusunda kayıt altına alınır ve gerektiğinde izlenir.

4.4. Donanım ve Yazılım Temini

- Üniversite bünyesinde kullanılacak donanım, yazılım ve bilgi teknolojileri hizmetlerinin temini, Üniversitenin satın alma ve tedarik süreçlerine uygun olarak gerçekleştirilir.
- Satın alınacak veya temin edilecek ürün ve hizmetlerde bilgi güvenliği, kişisel veri güvenliği, iş sürekliliği, hizmet sürekliliği ve kalite gereksinimleri dikkate alınır.
- Temin edilen donanım ve yazılımlar, gerekli kontroller gerçekleştirildikten sonra ilgili bilgi sistemlerinde kullanıma alınır.
- Kullanılan yazılımların lisans, bakım, destek ve güvenlik gereksinimleri ilgili birimler tarafından takip edilir.

4.5. Dış Kaynaklı ve Proje Kapsamındaki Varlıklar

- Dış kaynaklardan veya projeler kapsamında temin edilen bilişim ve diğer ilgili varlıklar, ilgili mevzuat ve Üniversitenin taşınır kayıt ve yönetim süreçlerine uygun şekilde kayıt altına alınır.
- Bu varlıkların sorumluluğu ilgili birim veya kişiye atanır.
- Dış kaynaklı varlıkların kullanımında bilgi güvenliği, kişisel veri güvenliği, iş sürekliliği ve hizmet yönetimi gereksinimleri dikkate alınır.

4.6. Fiziksel ve Taşınabilir Varlıkların Korunması

- Taşınabilir bilgisayar, mobil cihaz, harici disk, USB bellek ve benzeri varlıklar kayıp, hırsızlık, yetkisiz erişim ve kötüye kullanıma karşı korunur.
- Kişisel veri veya gizli bilgi içeren taşınabilir ortamlar için gerekli güvenlik önlemleri uygulanır.
- Varlıkların kurum dışına çıkarılması ve taşınması, ilgili yetkilendirme ve kullanım kurallarına uygun olarak gerçekleştirilir.

4.7. Varlıkların Kullanımdan Kaldırılması

- Kullanım ömrünü tamamlayan veya artık ihtiyaç duyulmayan varlıklar güvenli şekilde kullanım dışı bırakılır.
- Kullanımdan kaldırılan bilgi teknolojileri varlıklarında bulunan kişisel veriler, gizli bilgiler ve diğer kurumsal bilgiler; ilgili saklama ve imha kurallarına uygun şekilde silinir, yok edilir veya gerekli durumlarda anonim hale getirilir.
- Varlıkların imha, teslim veya devretme işlemleri ilgili kayıtlarla belgelendirilir.

4.8. Varlıkların Gözden Geçirilmesi

Varlık envanterleri ve varlık sahiplikleri;

- en az yılda bir kez,
- önemli sistem veya altyapı değişikliklerinde,
- yeni bir bilgi sistemi veya yazılım devreye alındığında,
- birim veya görev değişikliklerinde,
- varlıkların kullanımdan kaldırılması durumunda,
- önemli bilgi güvenliği veya iş sürekliliği olayları sonrasında gözden geçirilir ve gerekli güncellemeler yapılır.

5. YAPTIRIM

Bu politikada belirtilen kurallara aykırı hareket eden personel ve diğer yetkili kullanıcılar hakkında, fiilin niteliğine göre Üniversitenin ilgili mevzuatı, Disiplin Prosedürü, sözleşmeler ve diğer ilgili düzenlemeler kapsamında gerekli işlemler uygulanır.

Üçüncü taraflar ve hizmet sağlayıcılar açısından ise ilgili sözleşmelerde yer alan bilgi güvenliği, kişisel veri güvenliği, gizlilik ve diğer yükümlülükler uygulanır.