1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi (SDÜ) bilgi sistemleri ve bilgi varlıklarına erişimde kimlik doğrulama ve yetkilendirme kurallarını belirlemek; erişimlerin görev, yetki ve ihtiyaçlar doğrultusunda kontrollü olarak gerçekleştirilmesini sağlamaktır.

2. KAPSAM

Bu politika; SDÜ Entegre Yönetim Sistemi (EYS) kapsamında yer alan bilgi sistemleri, uygulamalar, veri tabanları, işletim sistemleri, ağ ve sunucu sistemleri ile bu sistemlere erişen SDÜ personeli, öğrencileri, hizmet sağlayıcılar ve diğer yetkili kullanıcıları kapsar.
Politika, SDÜ Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilindeki bilgi sistemlerine yönelik kimlik doğrulama, hesap yönetimi, erişim yetkilendirme ve ayrıcalıklı erişim süreçlerini kapsar.

3. SORUMLULUKLAR

- **Bilgi İşlem Daire Başkanlığı:** Merkezi kimlik doğrulama, kullanıcı hesapları ve erişim yetkilerinin teknik olarak yönetilmesinden sorumludur.
- **Birim yöneticileri:** Personelin görev ve sorumlulukları doğrultusunda erişim ihtiyaçlarının belirlenmesinden ve yetki taleplerinin onaylanmasından sorumludur.
- **Kullanıcılar:** Kendilerine tahsis edilen kullanıcı hesabı ve kimlik doğrulama bilgilerinin güvenliğinden ve yalnızca yetkileri kapsamında işlem yapmaktan sorumludur.
- **Sistem yöneticileri:** Sistemlerde tanımlanan erişim yetkilerinin uygulanması, izlenmesi ve gerekli kontrollerin gerçekleştirilmesinden sorumludur.

4. UYGULAMA

4.1. Kimlik Doğrulama ve Kullanıcı Hesapları

- SDÜ bilgi sistemlerine erişim sağlayacak kullanıcıların kimlikleri, kullanılan sistemin gerektirdiği uygun kimlik doğrulama yöntemi ile doğrulanır.
- Kullanıcılara mümkün olduğunca kişiye özel kullanıcı hesabı tanımlanır. Ortak kullanıcı hesaplarının kullanımı zorunlu haller dışında engellenir.
- Kullanıcı hesapları, personelin veya kullanıcının görev, sorumluluk ve erişim ihtiyacına göre oluşturulur ve yetkilendirilir.
- Kullanıcı hesapları yalnızca ilgili kişinin görevini yerine getirmesi için gerekli olan sistem ve kaynaklara erişim sağlayacak şekilde yapılandırılır.
- Görev değişikliği, birim değişikliği veya işten ayrılma durumlarında kullanıcının erişim yetkileri gözden geçirilir ve gerekli güncellemeler gerçekleştirilir.

4.2. Yetkilendirme ve Erişim Hakları

- Bilgi sistemleri, uygulamalar, veri tabanları, işletim sistemleri, ağ kaynakları ve diğer bilgi varlıkları üzerindeki kullanıcı rolleri ve erişim yetkileri belirlenir ve kontrol altında tutulur.
- Erişim yetkileri, görev gereği erişim ve en az yetki prensipleri doğrultusunda verilir.

- Kullanıcılara görevlerini yerine getirebilmeleri için gerekli olmayan ayrıcalıklı erişim hakları tanımlanmaz.
- Ayrıcalıklı erişim yetkileri sınırlı sayıda kullanıcıya verilir ve düzenli olarak gözden geçirilir.
- Erişim ve yetki seviyelerinin güncelliği belirlenen periyotlarda kontrol edilir. Görev veya sorumluluk değişikliklerinde ayrıca değerlendirme yapılır.
- Kullanıcıların yetki aşımına yönelik faaliyetleri izlenir ve tespit edilen yetki ihlalleri ilgili süreçler kapsamında değerlendirilir.

4.3. Kimlik Doğrulama Bilgileri

- Kullanıcılar kendilerine tahsis edilen parola ve diğer kimlik doğrulama bilgilerini gizli tutar ve başkalarıyla paylaşmaz.
- Kimlik doğrulama bilgileri kişiye özel olarak kullanılmalı ve başkasının hesabı üzerinden işlem yapılmamalıdır.
- Kullanılan sistemlerin teknik özellikleri ve risk seviyeleri dikkate alınarak güçlü parola, çok faktörlü kimlik doğrulama ve benzeri güvenli kimlik doğrulama yöntemleri uygulanabilir.
- Kullanıcı hesabının veya kimlik doğrulama bilgilerinin yetkisiz kişilerce kullanıldığından şüphe edilmesi durumunda ilgili birime bildirim yapılır ve gerekli güvenlik önlemleri alınır.

4.4. Erişim Kayıtları ve İzleme

- Bilgi sistemlerine yönelik başarılı ve başarısız erişim girişimleri, sistemin teknik özellikleri ve kayıt politikaları doğrultusunda loglanır.
- Tekrarlanan başarısız oturum açma girişimleri ve olağandışı erişim hareketleri incelenir.
- Ayrıcalıklı kullanıcı hesaplarının faaliyetleri, bilgi güvenliği gereklilikleri doğrultusunda izlenir ve kayıt altına alınır.
- Erişim kayıtları yetkisiz değişiklik, silme veya erişime karşı korunur.

4.5. Kullanıcı Rolları ve Yetki Seviyeleri

Kullanıcıların erişim yetkileri personel unvanına göre otomatik olarak belirlenmez. Yetkilendirme, kullanıcının görev ve sorumlulukları, erişim ihtiyacı, bilgi varlığının sınıflandırması ve ilgili birimin onayı dikkate alınarak gerçekleştirilir.

Domain Rolü	**Yetkisi**
Sistem Yöneticisi	Sistem yönetimi ve gerekli ayrıcalıklı erişim yetkilerine sahip
Yönetici	Bilgisayarının Yerel Yöneticisi
Akademik Personel	Bilgisayar Yerel Yöneticisi (Sistem ve Network Ayarlarını Değiştiremez, Denetim Masasına Müdahalede Bulunamaz)
Daire Başkanı	Bilgisayar Yerel Yöneticisi (Sistem ve Network Ayarlarını Değiştiremez, Denetim Masasına Müdahalede Bulunamaz) Birim içi depolama alanını yönetebilir.
İdari Personel	USB Veri Depolama Aygıtlarını kullanamaz. Program yükleme ve kaldırma yetkisi yoktur. Sistem ayarlarını değiştiremez ve Denetim masasına erişemez.

İşçi, Geçici İşçi ve Sözleşmeli Personel	USB Veri Depolama Aygıtlarını kullanamaz. Program yükleme ve kaldırma yetkisi yoktur. Sistem ayarlarını değiştiremez ve Denetim masasına erişemez. Yaptıkları işe göre yetkilendirilen programlar dışında herhangi bir program kullanımı gerçekleştiremez.
Öğrenci	USB Veri Depolama Aygıtlarını kullanamaz. Program yükleme ve kaldırma yetkisi yoktur. Sistem ayarlarını değiştiremez ve Denetim masasına erişemez

Kullanıcılara tanımlanan erişim yetkileri, görev değişikliği, birim değişikliği, işten ayrılma veya erişim ihtiyacının ortadan kalkması durumlarında güncellenir veya kaldırılır.

4.6. Ayrıcalıklı Erişimler

- Sistem yöneticisi, veritabanı yöneticisi, ağ yöneticisi ve benzeri ayrıcalıklı hesaplar yalnızca yetkilendirilmiş personele tanımlanır.
- Ayrıcalıklı hesapların kullanımı gerektiğinde kişiye özel hesaplar üzerinden gerçekleştirilir.
- Ayrıcalıklı erişim hakları düzenli olarak gözden geçirilir.
- Ayrıcalıklı erişimlerin kullanımına ilişkin kayıtlar, ilgili sistemin özellikleri ve bilgi güvenliği gereklilikleri doğrultusunda tutulur.

4.7. Yetki İhlalleri

Yetkisiz erişim, hesap paylaşımı, yetki aşımı veya kimlik doğrulama bilgilerinin uygunsuz kullanımı tespit edildiğinde ilgili bilgi güvenliği süreçleri işletilir ve gerekli idari ve teknik tedbirler alınır.

5. YAPTIRIMLAR

Bu politikaya aykırı hareket eden SDÜ personeli ve diğer kullanıcılar hakkında ilgili mevzuat, SDÜ düzenlemeleri ve yürürlükteki disiplin hükümleri doğrultusunda işlem yapılır. Yetkisiz erişim veya güvenlik ihlali tespit edilmesi halinde ilgili kullanıcının erişim yetkileri geçici veya kalıcı olarak sınırlandırılabilir ya da kaldırılabilir.