1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında geliştirilen, temin edilen veya mevcut yazılımlarda yapılan değişikliklerin güvenli yazılım geliştirme ilkelerine uygun olarak analiz, tasarım, geliştirme, test, devreye alma ve işletim süreçlerinin yürütülmesine ilişkin temel kuralları belirlemektir.

2. KAPSAM

Bu politika;

- Süleyman Demirel Üniversitesi Daire Başkanlıkları,
- Genel Sekreterliği,
- Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimini,
- Bilgi İşlem Daire Başkanlığı ve Hastanesi Bilgi İşlem Birimini tarafından geliştirilen yazılımları,
- Kurum adına geliştirilen veya kurumsal bilgi sistemlerinde kullanılan yazılımları,
- Yazılım geliştirme, bakım, güncelleme, entegrasyon ve değişiklik faaliyetlerini kapsar.

3. SORUMLULUKLAR

3.1. Bilgi İşlem Daire Başkanlığı ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimini

Yazılım geliştirme süreçlerinin bu politika ve ilgili EYS dokümanlarına uygun olarak yürütülmesinden sorumludur.

3.2. Yazılım ve Web Geliştirme Birimi

- Yazılım geliştirme yaşam döngüsünün güvenli şekilde yürütülmesinden,
- Kaynak kodların güvenliğinin sağlanmasından,
- Yazılım geliştirme ve test faaliyetlerinin gerçekleştirilmesinden,
- Güvenlik açıklarının ve yazılım kaynaklı risklerin değerlendirilmesinden,
- Test sonuçlarının kayıt altına alınmasından,
- Yazılımların işletim ortamına güvenli şekilde aktarılmasından sorumludur.

3.3. Proje Yöneticisi / Proje Ekibi

- Yazılım gereksinimlerinin belirlenmesi,
- Proje planının oluşturulması,
- Görev ve yetkilerin belirlenmesi,
- Geliştirme, test ve devreye alma faaliyetlerinin koordinasyonu,
- Risklerin ve güvenlik gereksinimlerinin değerlendirilmesi konularından sorumludur.

3.4. Yazılım Kullanıcıları ve İlgili Birimler

Yazılımın iş gereksinimlerinin belirlenmesine, test edilmesine ve kabul süreçlerine ilgili görev ve yetkileri kapsamında katkı sağlar.

4. UYGULAMA

4.1. Analiz ve Gereksinimlerin Belirlenmesi

Yazılım geliştirme sürecinin başlangıcında;

- Yazılımın amacı, kapsamı ve işlevsel gereksinimleri belirlenir.
- Bilgi güvenliği gereksinimleri değerlendirilir.
- Gerekiyorsa kişisel verilerin işlenmesine ilişkin gereksinimler belirlenir.
- Yazılımın kullanacağı veri tabanı, sunucu, işletim sistemi ve diğer teknik gereksinimler belirlenir.
- Kullanıcı ve sistem erişim yetkileri belirlenir.
- Kullanılacak web servisleri, API'ler ve diğer entegrasyonlar belirlenir.
- İç ve dış paydaşlardan veri alınması veya veri paylaşılması gerekiyorsa gerekli yetki ve izinler ilgili süreçler kapsamında alınır.
- Kullanılacak programlama dili, geliştirme araçları ve teknik mimari belirlenir.
- Proje yöneticisi veya proje ekibi belirlenir.
- Proje için gerekli iş takvimi ve sorumluluklar oluşturulur.

Yazılımın kişisel veri işlemesi durumunda, gerekli görülmesi halinde KVYS kapsamında ilgili gizlilik ve veri koruma gereksinimleri değerlendirilir.

4.2. Tasarım

Analiz aşamasında belirlenen gereksinimler doğrultusunda yazılımın teknik ve işlevsel tasarımı oluşturulur.

Tasarım aşamasında;

- Uygulama mimarisi,
- Veri tabanı yapısı,
- Kullanıcı ve yetki modeli,
- Kimlik doğrulama ve erişim kontrol mekanizmaları,
- Veri aktarım yöntemleri,
- Loglama ve izleme gereksinimleri,
- Yedekleme ve kurtarma gereksinimleri,
- Kişisel verilerin korunmasına ilişkin gereksinimler,
- Güvenlik açıklarının önlenmesine yönelik kontroller değerlendirilir.

4.3. Geliştirme

Geliştirme faaliyetleri sırasında;

- Belirlenen yazılım mimarisi ve güvenlik gereksinimlerine uygun kodlama yapılır.
- Kaynak kodlara erişim yetkileri görev ve sorumluluklara göre sınırlandırılır.
- Kaynak kodların yetkisiz değiştirilmesine karşı gerekli erişim kontrolleri uygulanır.
- Kaynak kod ve proje dosyalarının uygun şekilde yedeklenmesi sağlanır.
- Kullanılan üçüncü taraf kütüphane, framework, paket ve yazılım bileşenlerinin güvenilirliği ve güncelliği değerlendirilir.
- Güvenlik açığı bulunan veya desteklenmeyen yazılım bileşenlerinin kullanılması önlenir.
- Yazılım bileşenlerinde değişiklik yapılmadan önce gerekli yedekleme ve değişiklik kontrolü gerçekleştirilir.
- Parola, API anahtarı, erişim anahtarı ve benzeri gizli bilgiler kaynak kod içerisinde açık şekilde tutulmaz.
- Gerektiğinde güvenli kod analizleri ve güvenlik kontrolleri gerçekleştirilir.

4.4. Geliştirme, Test ve İşletim Ortamlarının Ayrılması

Yazılım geliştirme, test ve işletim faaliyetleri mümkün olduğunca ayrı ortamlarda gerçekleştirilir.

Geliştirme ve test faaliyetleri sırasında işletim ortamındaki gerçek verilerin doğrudan kullanılması önlenir.

Zorunlu olarak gerçek verilerin test ortamında kullanılması gereken durumlarda;

- Veri güvenliği değerlendirilir,
- Kişisel veriler mümkün olduğunca anonimleştirilir veya uygun yöntemlerle maskelenir,
- Erişimler sınırlandırılır,
- Veriler yalnızca gerekli olduğu süre boyunca kullanılır,
- Test tamamlandığında test verileri uygun şekilde silinir veya imha edilir.

4.5. Test

Test aşamasında geliştirilen yazılımın belirlenen gereksinimleri ve güvenlik kriterlerini karşılayıp karşılamadığı değerlendirilir.

Gerekli durumlarda;

- Fonksiyonel testler,
- Entegrasyon testleri,
- Performans testleri,

- Güvenlik testleri,
- Kullanıcı kabul testleri gerçekleştirilir.

İlk testler proje ekibi tarafından geliştirme veya test ortamında gerçekleştirilir.

Tespit edilen hatalar ve güvenlik açıkları giderilmeden yazılımın işletim ortamına alınmaması esastır.

Kullanıcı kabulü gereken uygulamalarda, yetkili kullanıcılar tarafından kabul testleri gerçekleştirilir ve test sonuçları kayıt altına alınır.

4.6. Pilot Uygulama ve Kullanıcı Kabulü

Gerekli görülen yazılımlar işletim ortamına tamamen açılmadan önce sınırlı kullanıcı veya pilot birim üzerinde kullanıma sunulabilir.

Pilot uygulama sırasında;

- Kullanıcı yetkileri sınırlandırılır.
- Kullanıcılara gerekli bilgilendirme yapılır.
- Geri bildirimler alınır.
- Tespit edilen hata ve güvenlik sorunları giderilir.
- Gerekli görülmesi halinde kullanıcı kabulü gerçekleştirilir.

4.7. İşletime Alma

Test ve kabul aşamalarının tamamlanmasından sonra yazılım, yetkilendirilmiş personel tarafından işletim ortamına alınır.

İşletime alma işlemleri;

- Yetkilendirilmiş kişiler tarafından,
- Onaylanmış değişiklik kapsamında,
- Belirlenen zaman planına uygun olarak,
- Gerekli yedekleme ve geri dönüş planları dikkate alınarak gerçekleştirilir.

4.8. Değişiklik Yönetimi

İşletimde bulunan yazılımlarda yapılacak değişiklikler ilgili değişiklik yönetimi süreci kapsamında gerçekleştirilir.

Değişiklikler;

1. Talebin oluşturulması,

2. Etki ve risk değerlendirmesinin yapılması,
3. Gerekli onayların alınması,
4. Geliştirme ve test işlemlerinin gerçekleştirilmesi,
5. Değişikliğin işletim ortamına aktarılması,
6. Sonuçların kontrol edilmesi aşamaları dikkate alınarak yürütülür.

Acil değişiklikler, kurumun ilgili değişiklik yönetimi kurallarına uygun olarak gerçekleştirilir ve sonrasında kayıt altına alınır.

4.9. Web Servisleri ve Entegrasyonlar

Kurum içi veya kurum dışı sistemlerle veri alışverişi sağlayan web servisleri ve API'ler için;

- Yetkilendirme ve kimlik doğrulama mekanizmaları uygulanır.
- Veri aktarımının güvenliği sağlanır.
- Gereksiz veri aktarımı yapılmaz.
- Veri paylaşımının hukuki, idari ve teknik gereksinimleri değerlendirilir.
- Kişisel veri içeren veri aktarımında KVYS kapsamında belirlenen gereksinimler dikkate alınır.
- Servis erişimleri ve yetkileri gerektiği ölçüde sınırlandırılır.

4.10. Kaynak Kod ve Yazılım Varlıklarının Korunması

Kaynak kodlar ve yazılım geliştirme süreçlerine ilişkin diğer bilgiler yetkisiz erişim, değiştirme, silme ve ifşaya karşı korunur.

Kaynak kod depolarına erişimler görev ve sorumluluk esasına göre yetkilendirilir ve gerekli durumlarda erişim kayıtları tutulur.

Personelin görev değişikliği veya kurumdan ayrılması halinde ilgili erişim yetkileri gözden geçirilir ve gerekli yetkiler kaldırılır.

4.11. Yazılım Güvenlik Açıkları

Geliştirilen veya işletilen yazılımlarda tespit edilen güvenlik açıkları değerlendirilir ve önem derecesine göre giderilir.

Güvenlik açıklarının yönetiminde Zaafiyet ve Yama Yönetimi Politikası ve ilgili EYS süreçleri dikkate alınır.

5. YAPTIRIM

Bu politikada belirtilen kurallara aykırı gerçekleştirilen faaliyetler, ilgili EYS süreçleri kapsamında uygunsuzluk olarak değerlendirilir.

Gerektiğinde yürürlükteki mevzuat, kurum düzenlemeleri ve Disiplin Prosedürü hükümleri doğrultusunda işlem yapılır.