



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

1. AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesine Bilgi İşlem Daire Başkanlığı uyum kurallarını oluşturmayı amaçlar.

2. KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesinin Bilgi İşlem Daire Başkanlığı uyum kurallarını kapsar.

3. SORUMLULAR

- Bilgi İşlem Daire Başkanlığı

4. TANIMLAR

5. UYGULAMA

5.1 Uygulama Tabanlı Olmayan Bilişim Sistemleri'nin Bakımı

5.2 Uygulama Geliştirme Prosedürleri

Uygulama geliştirme için standart bir süreç oluşturmadaki amaç yüksek kaliteli ve güvenli bir yazılımı en verimli ve en etkin şekilde tasarlayabilmek, geliştirebilmek ve sürekliliğini sağlayabilmektir. Uygulama geliştirme çalışmalarının maliyet, kaynak gereksinimi, iş süreçleri kriterleri dikkate alınarak proje olup olmadığı proje yöneticileri tarafından karar verilir. Yöntemdeki her faz, geliştirmenin bir sonraki fazına girdi oluşturacaktır. Bir sonraki faza geçmeden önce her fazın eksiksiz ve doğru olduğu kontrol edilir. Geliştirme yöntemi aşağıdaki fazlardan oluşur:

5.2.1 Planlama ve Fizibilite Çalışması

En başta yapılacak olan, proje kararı verildiğinde projeyi başlatacak, bir proje yöneticisi ve ilgili süreç sahiplerinden oluşan bir ekibin kurulmasıdır. Proje yönetimi başlangıç planlaması ve fizibilite çalışmasını gerçekleştirir. Bu ekip geliştirilmesi gereken sistemi bütünüyle ve detaylarıyla anlamaya çalışır. Edinilen bilgiye göre, aşağıdaki hususları içeren kapsamlı bir proje planı hazırlanır:

- Projenin kilit fazları ve hedefleri
- Hedeflere ulaşmak ve projeyi sonlandırmak için planlanan tarihler
- Projenin fazlarını bitirmek için gerekli kaynaklar
- Proje sırasında yapılması gereken dokümantasyon

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

5.2.2 Sistem Analizi ve Gereksinimlerinin Tanımı

Yazılım geliştirmenin bu fazındaki amaç, mevcut sistemi analiz etmek ve iş süreci sahibinin gereksinimlerini anlamaktır. Gereksinimleri belirlemek için tayin edilmiş ekip, iş süreci sahipleriyle görüşerek eksiksiz, anlamı açık ve kolay anlaşılabilir bir mevcut durum dokümanı hazırlanır. Mevcut durumun süreç sahipleri tarafından onayından sonra teknik yapıyı da içeren kavramsal tasarım dokümanı oluşturulur. Kavramsal tasarım dokümanı, her fazdaki gereksinimin izlenebildiği bir yapıda olacaktır. Bu fazdaki en kritik konu, ekibin iş süreci sahibiyle oturup ana güvenlik gereksinimlerini belirleme gerekliliğidir. Bu gereksinimler üzerinde iş süreci sahipleri ile karşılıklı anlaşılır.

Kavramsal tasarım dokümanı şunları içerir:

- İşlevsel gereksinimler
- Güvenlik gereksinimleri
- Kullanıcı Ara yüzü gereksinimleri
- Sözleşme / Yönetmelik / Yasa gereksinimleri
- Diğer özellikler – Tekrar kullanılabilirlik, Sürdürülebilirlik, Taşınabilirlik, Geliştirilebilirlik (genişletilebilirlik) vs.

Bunlar, gereksinimlerin belirlendiği bu faz süresince güvenlik gereksinimlerinin eksiksiz olarak belirlendiğinin ve dokümante edildiğinin kontrolü için İş Birimi Yöneticisi tarafından gözden geçirilir ve onaylanır.

5.2.3 Girdi Verisinin Doğrulanması

- Kapsamda belirlenenin üzerinde ortaya çıkan değerler, veri alanlarındaki geçersiz karakterler, kayıp veya eksik veri, alt ya da üst veri sınırlarının aşımı ve yetkisiz veya tutarlı olmayan kontrol verisi gibi hataların tespiti için girdi kontrolleri
- Geçerliliklerinin ve bütünlüklerinin kontrol edilmesi için kilit alanların veya veri dosyalarının içeriğinin periyodik olarak gözden geçirilmesi
- Sistem doğrulamalarında oluşan hatalarının tespiti sonrasında uygulanması gereken iyileştirme faaliyetleri
- Veri giriş sürecine dâhil olan tüm kullanıcıların sorumluluklarının tanımlanması

5.2.4 Veri İşlemenin Kontrol Edilmesi

Verinin değiştirilmesi için kullanılan ekle ve sil fonksiyonlarının ara yüzde kullanımı ve ekran tasarımlarındaki yerleri belirlenir. Programların yanlış sırada çalıştırılmasını veya hatalı bir ön işlem sonrasında çalışmasını engellemeye yönelik yapı kurulur.

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

5.2.5 Mesajların Doğrulanması / Şifrelenmesi

Önemli elektronik şartnameler, sözleşmeler, teklifler veya diğer benzer elektronik veri paylaşımları gibi, güvenlik açısından mesaj içeriği bütünlüğünün korunmasının gerekli olduğu durumlarda mesaj doğrulanması yapılır.

5.2.6 Çıktı Verisinin Doğrulanması

- Çıktı verisinin anlamlı olduğunun test edilmesi için gerekli mantık kontrolleri
- Çıktı doğrulama testleri sonrasında uygulanması gereken faaliyetler
- Veri çıkış sürecine dâhil olan tüm personelin sorumluluklarının tanımlanması

5.2.7 Sistem Tasarımı

Bir yazılım tasarımı, geliştirilecek yazılım ürünlerinin anlamlı bir mühendislik sunumudur. Tasarımın, gereksinimleri karşılar nitelikte olduğu kontrol edilir ve kalite standartlarının daha önce belirlenen kriterleri karşılaması sağlanır. Tasarım fazında geçerli olduğu sürece dört ana konu incelenir ve tasarlanır: veri, yapı, ara yüzler ve bileşenler. Bu fazda aşağıdaki dört tasarım modeli hazırlanır:

Veri Tasarımı – Yazılımda uygulanacak veri yapılarının detayı

Yapı & Bileşen Tasarımı – Yazılım gereksinimlerini karşılamak için gerekli ana yapı ve prosedürel bileşenlerin detayı

Arayüz Tasarımı – Yazılım bileşenlerinin kendi aralarında ve diğer sistemlerle nasıl haberleşeceğinin detayları. Geliştirme ve kodlamanın temelini oluşturacak bu fazda yukarıdaki dört modelin kapsamlı tasarım dokümanları oluşturulur.

5.2.8 Geliştirme - Kodlama

Tasarım dokümanı, yazılımcıların kodlamasını yapacağı yazılım için temel oluşturacaktır. Her bir prosedür / modül, teknik ekibe verilen özelliklere göre geliştirilir. Bu süreç programların ve yardımcı programların tasarlanmasını ve kodlanmasını, tablo ve veri elemanlarının yaratılmasını içerir. Yazılımcılara, güvenli kodlar geliştirmelerine destek olması için, yazılım dili / platformuna özel, güvenli kodlama adımları izlenir. Programlama esnasında şu koşullardan kaçınılır:

- Arabellek (buffer) aşımaları
- Geçici dosyaların uygun şekilde yönetilememesi
- Fazla karmaşık ve gereksiz kod
- Güvenli olmayan sistem çağrıları ve sistemler arası geçiş
- Şifrelerin ve yetki nesnelerinin kodun içine gömülmesi

Program geliştirme esnasında şu ana esaslara uyulur:

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

- Güvenilir programlar veya scriptler güvenilir olmayan program veya scriptleri çalıştıramaz.
- Bir script ya da program içerisinde, dosyanın sahibini ve dosya üzerinde tanımlı yetkileri kontrol ederken dosya ismi kullanılmaz. Bunun yerine dosya isimlerinin tutulduğu ayrı bir dosyanın ismi kullanılır (file handles).
- Değişkenler, diziler ve argümanlar kullanılırken, arabellek aşımının engellenmesi için kısıt / boyut kontrolleri uygulanır.
- Alt program akışları ve alt scriptler ortam değişkenlerini diğer script veya dosyalardan alamaz.
- Tüm kullanıcı girdileri zararlı kod içermelerine yönelik kontrol edilir.
- Bir program tarafından oluşturulan geçici dosyalar bu dosyalara olan gereksinim ortadan kalktığında silinir.

5.2.9 Test

Birim testleri

Birim testinin amacı, geliştirilen programın fonksiyonel ve teknik tasarım gereksinimlerini karşıladığını ve tüm işlemlerin, veritabanı güncellemelerinin ve işlevselliğin doğru sırayla ve uygun şekilde gerçekleştiğini kontrol etmektir. Bu test çeşitli senaryolar için programcı tarafından gerçekleştirilir. Programcı, tüm test senaryolarını, test koşullarını ve beklenen / gözlemlenen sonuçları da içeren test planını gözden geçirir. Testler, kod içerisinde tanımlı tüm fonksiyonların ve mantıksal yolların testini içerir ve tüm normal, beklenmeyen ve hata işleme (hem program girdileri hem de oluşabilecek çıktılar için) koşullarını ele alır.

Entegrasyon ve kabul testleri

Entegrasyon ve kabul testleri, süreç sahipleri ve/veya anahtar kullanıcılar tarafından modüllerin/süreçlerin birbirleri ile bağlantıları test edilir.

Bu fazda, ilgili proje Yöneticisi tüm güvenlik gereksinimlerinin programlarda uygulanıp uygulanmadığını test eder.

Bu fazda şu gereksinimler test edilir:

- Fonksiyonel gereksinimler
- Güvenlik gereksinimleri
- Kullanıcı ara yüzü gereksinimleri
- Sözleşme / Yönetmelik / Yasa gereksinimleri
- Diğer özellikler – Tekrar kullanılabilirlik, Sürdürülebilirlik, Taşınabilirlik, Geliştirilebilirlik (büyütülebilirlik) vs.

İş süreci sahipleri veya operasyon ekibi, tüm gereksinimler karşılanıyorsa test kabulünü onaylar. Herhangi bir hata mevcutsa, programdaki bu hataların giderilmesi için gerekli değişiklikler yapılır.

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

5.2.10 Operasyon Yazılımının Kontrol Edilmesi

Operasyonlardan sorumlu Bilgi İşlem personeli tarafından yazılımının canlı sisteminde yönetimi için aşağıdaki prosedürler uygulanır:

- Program kütüphanelerinin güncellenmesi, sadece uygun şekilde yetkilendirilmiş bu işe atanan yetkin personel tarafından gerçekleştirilir.
- Mümkün olan yerlerde canlı sistemler yalnızca çalıştırılabilir kod (executable) içerir.
- Testlerin başarılı olduğu belgelenmeden ve kullanıcı kabulü temin edilip ilgili program kaynak kütüphaneleri güncellenmeden çalıştırılabilir kodlar işletim sistemlerinde çalıştırılmaz.
- Program kütüphanelerinin tüm güncellemeleri için denetim kaydı tutulur.
- Beklenmedik bir durum için yazılımın önceki tüm sürümleri saklanır.
- Operasyonda kullanılan ve tedarikçiden temin edilen yazılımın bakımı tedarikçinin desteği alınarak yapılır. Programı yeni bir sürüme yükseltme kararı, bu sürümü etkileyecek yeni güvenlik konuları ve güvenlik problemlerinin sayısı ve kritikliği göz önünde bulundurularak verilir.
- Yazılım yamaları güvenlik zayıflıklarını azaltabilecekleri ya da ortadan kaldıracabilecekleri durumda uygulanır.

5.2.11 Sistem Test Verisinin Korunması

Test verisi canlı ortam verisi ile mümkün olduğunca aynı tutulur. Aktarım tarihi, test amacıyla kullanılmadan önce kontrol edilir. Test ortamına erişim hakkı uygulama testine dahil edilen personele tanınır.

5.2.12 Canlı Ortama Aktarım

Uygulama testi başarılı olduğunda, uygulama canlı sistem ortamına aktarılır. Proje yöneticisi, entegrasyon ve kabul testlerinin sonuçlarını gözden geçirdikten sonra uygulamanın canlı ortama aktarılması için onay verir. Canlı ortama geçişten önce, tüm sistemlerde program geliştirme planında belirtilen mantıksal erişim kontrollerinin uygulanıyor olması gerekir. Test ortamı ve test verisine erişim canlı sistemde tanımlanan yetkilere mümkün olduğunca aynı yetkilere sahip test kullanıcıları tarafından sağlanır.

5.2.13 Geliştirme, Test ve Canlı Ortamı

Geliştirme, test ve canlı ortamları fiziksel ve mantıksal olarak birbirlerinden olabildiğince ayrılır. Ortam ilk defa yaratıldığında ve yazılımın her ortama ilk yüklenişinde, Bilgi İşlem veya proje yöneticisinin onayı alınır. Bundan sonra, mevcut ortamlarda yapılan her değişikliği ilgili Bilgi İşlem veya proje yöneticisi onaylar. Canlı ortamda oluşturulan erişim kontrol ortamının aynısı test ortamında da oluşturulur.

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

5.2.14 Program Kaynak Koduna Erişimin Kontrol Edilmesi

Bilgi İşlem yöneticisi kaynak kodunu yetkisiz erişimlere karşı korumak için aşağıdaki prosedürleri uygular.

- Mümkün olan ortamlarda, program kaynak kütüphaneleri işletim sistemlerinde tutulur.
- Program kütüphanesinden sorumlu personel, program kaynak kütüphanelerine sınırsız erişime sahip olamaz.
- Geliştirilmekte ya da bakımda olan programlar, canlı ortam kaynak kütüphanelerinde tutulamaz.
- Program listeleri güvenli bir ortamda saklanır.
- Program kaynak kütüphanelerinin değiştirilmesi ve kopyalanması Değişiklik Kontrolü Prosedürleri'ne göre gerçekleştirilir.
- Bilgi Güvenliği Yöneticisi, Bilgi İşlem personelinin bu prosedürlere uyup uymadığını altı ayda bir defa gözden geçirir.

5.3 Konfigürasyon Yönetimi Prosedürleri

Değişiklik kontrol süreci, ağ ekipmanlarındaki ve ağ ile ilgili projelerin yanı sıra yazılım ve yazılım projelerindeki değişiklikleri yönetmeye yardımcı faaliyetlerin tanımlanması ve dokümanite edilmesini içerir. Konfigürasyon Yönetim Süreci, bir yazılımın veya ekipmanın çeşitli zamanlardaki fonksiyonel ve fiziksel özelliklerinin doğru bir şekilde tutulabilmesini sağlar. Ayrıca, bir CI (Konfigürasyon Ögesi - Configuration Item) yaşam döngüsü çerisinde operasyon yazılımının ve ekipmanların bakım esnasında bütünlüğünü ve izlenebilirliğini sağlamak için belirlenen özellikler üzerinde yapılan değişikliklerin sistematik kontrollerinin gerçekleştirilmesine yardımcı olur. Süreç aynı zamanda değişikliklerin izlenme gereksinimlerini tanımlar ve yazılımın son halinin, yani sürümün planlanan iyileştirmeleri içerdiğini doğrulama imkânı sunar.

Her bir proje ve operasyonel yazılımın bakımı için özel Konfigürasyon Yönetimi süreçleri tanımlanır. Projenin başında oluşturulan proje ekibi konfigürasyon yönetimi prosedürlerini belirler ve uygular. Operasyonel yazılımın bakımı için, konfigürasyon yönetimi prosedürlerini Bilgi İşlem yöneticisi belirler ve uygulanmasını sağlar.

5.3.1 Konfigürasyonun Belirlenmesi

Yazılımlar ve ağ donanımları genel olarak birçok bölüm veya parçadan oluşurlar. İlgili dokümantasyon da dâhil olmak üzere bu yazılımların ve donanımların her parça ve bölümü konfigürasyon ögesi olarak adlandırılabilir. Proje ekibi bir projedeki tüm konfigürasyon öğelerini, Bilgi İşlem yöneticisi ise operasyon içerisindeki tüm konfigürasyon öğelerini belirler.

Bir projedeki öğeler (CI) – Örnek	Operasyon öğeleri (CI) - Örnek
Proje Planı	Kaynak Kodu
Gereksinim Detayları	Çalıştırılabilir Dosyalar

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

Tasarım Dokümanı Kod Çalıştırılabilir Dosyalar Test Planları Test Stratejileri Geliştirmeler – Sürümler	Kullanıcı Dokümantasyonu Kurulum Dokümantasyonu Ağ Ekipmanları (Aktif ekipman konfigürasyonları ve pasif ağ elementleri)
--	---

Sürüm_Kontrolü

CI'nın herhangi bir zamanda sistemdeki bulunduğu durum temel olarak adlandırılır. Temel noktası geliştirme veya operasyonel yaşam döngüsünde bir referans noktası olarak görev yapar. Her yeni temel noktasının değeri bir geçmiş temel değeri ile CI üzerinde yapılan bir dizi onaylanmış değişikliğin birlikteliğinden oluşur.

Herhangi bir zaman aralığında bir referans değeri oluşturulabilir. Referans değeri versiyon '1.0' veya tedarikçi tarafından verilen herhangi bir versiyon numarası ile başlar. Yapılandırılabilir öğedeki minör bir değişiklikte, versiyon numarasının ondalık hanesi bir arttırılır (örn. eski versiyon '1.1' ise yenisi '1.2' olacaktır). CI'da majör bir değişiklik varsa, ana versiyon bir arttırılır (örn. versiyon '1.1'den '2.1'e yükseltilir). Operasyon yazılımı ve ekipmanlar için, versiyon tedarikçinin ya da hizmet sağlayıcının sağladığı şekliyle korunur.

Her bir proje veya operasyon kapsamındaki yazılım veya ekipman için ekipten bir kişi kütüphane sorumlusu olarak seçilir. Bu kişi bir projenin ya da operasyon yazılımının, nesne ve kaynak programları ve program adını, eski versiyon numarasını, büyüklüğünü (kodun satır sayısı, program dosyasının bayt olarak kapladığı yer, ekipman marka ve modelleri), son güncelleme tarihini ve yeni versiyon numarasını içeren modüller de dâhil tüm yapılandırılabilir öğelerin bakımından sorumludur.

5.3.2 Konfigürasyon Kontrolü

Onaylanan değişikliklerin karara bağlanması, ilgili CI'lar için koordine edilmesi ve uygun temel değerleri üzerine uygulanmasına Konfigürasyon Kontrolü denir. Konfigürasyon kontrolü "Program Değişikliği"nin Bilgi İşlem yöneticisi tarafından onaylanmasından sonra veya bir operasyon yazılımı canlıya geçirileceği zaman gündeme gelir. "Program Değişikliği" onayının ardından şu prosedür izlenir:

ÇIKIŞ (Değişiklik için CI'nın kilitleyerek dışarı alınması)

Program değişikliği onaylandıktan sonra, ilgili geliştirme ekibi değiştirilmesi gereken CI'yı belirler ve kütüphane sorumlusunu bilgilendirir

Aynı şekilde, operasyon ekibi de bir operasyon yazılımının yeni bir versiyonunu uygulamak için kütüphane sorumlusunu bilgilendirir.

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

Giriş

Değiştirilen birimin uygulamaya alınmasından önce geliştirmeci birimi tamamen test eder. Geliştirmeci aynı zamanda, eğer mevcutsa, değiştirilen birim ile ilgili diğer dokümanları da sağlar (tasarım dokümanı, test dokümanı vs). Değiştirilen öge için yazılım tarafından yeni bir versiyon numarası tayin edilir. Değişiklik tarihi, ögenin çıkışını talep eden kişi, uygulamaya alan kişi ve değişiklik tanımı konfigürasyon yönetimi aracında dokümante edilir.

Operasyon yazılımı, tedarikçi veya 3. parti geliştirmeciler tarafından yeni bir versiyon çıkarıldığında uygulamaya alınır. Yeni versiyon, test ortamında test edilip, gerçekleştirilen testler Bilgi İşlem yöneticisi tarafından gözden geçirilip onaylandıktan sonra uygulamaya alınır.

Sürüm

Program değişikliği gerçekleştiğinde, yazılım için yeni bir temel oluşur ve değiştirilen birimler (CI) ve diğer ilgili birimler yeni bir yazılım sürümü geliştirilmesi için dışarı alınır.

Benzer şekilde, operasyon yazılımı için de, Bilgi İşlem yöneticisinin onayından sonra üretim ortamında uygulanması için yeni bir yazılım sürümü çıkarılır.

Yeni bir sürüm çıkarıldığında kütüphane sorumlusu, eski sürüm üzerinde yapılan tüm değişikliklerin yeni sürümün oluşturulması için kullanıldığından emin olmak için sürümü kontrol eder.

5.3.3 Konfigürasyonun Gözden Geçirilmesi

Yeni sürüm çıkarıldıktan sonra Sistem Yöneticisi veya Bilgi İşlem Yöneticisi çıkarılan yeni sürümü gözden geçirir ve planlanmış ve onaylanmış değişikliğin uygulanması için gerekli tüm konfigürasyon birimi yeni versiyona dâhil edildiğini kontrol eder. Bu süreç yazılımdaki tüm fonksiyonel tarafın (beklentilerin) tamamlandığının ve program, dokümantasyon ve verinin doğru aktarımının gerçekleştirildiğini doğrular. Gözden geçirmenin ardından, yeni versiyon resmi olarak (proje ekibindeki yetkili personel tarafından üretim ortamında uygulanması için) çıkarılabilir.

5.4 Program Değişikliği Kontrolü Prosedürleri

5.4.1 İlk Kullanıcı Talebi

Bir uygulama programında düzeltme / değişiklik / yeni fonksiyonellik gerekiyorsa, kullanıcı gereksinimleri Yardım Masasına iletilir. Değişiklik talebi ilgili personel tarafından yardım masası altyapısı üzerinden yapılır. Gereksinim, örneğin mevcut fonksiyondaki yazılım hatalarına, sık karşılaşılan, programın bazı bölümlerinin hatalı olduğunu işaret eden hata mesajlarına, sisteme ya da raporlamaya eklenmesi gereken ek özelliklere, kanunların zorunlu tuttuğu değişikliklere yönelik olabilir. Yazılım ekibi kaynak kodlarında yapılacak değişiklikler için yardım masası aracında değişiklik kaydı açar.

Her bir uygulama değişikliği talebi için ilgili sürece ilişkin adlandırma kullanılır. Bu kural ilgili uygulamanın adını, modül adını belirtir ve ayrımı sağlayacak şekilde numaralandırılır.

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

5.4.2 Talep ve Sınıflandırmanın Analizi

Bilgi İşlem yöneticisi ve proje yöneticisi, onaylamadan önce değişiklik talebini inceler. Bu inceleme için, Bilgi İşlem yöneticisi ve proje yöneticisi, İş Süreci Sahipleri'nden ve Sistem Yöneticileri'nden yardım alabilir. Talebin analizi talebi karşılayan Bilgi İşlem personeli veya geliştirme ile ilgili olarak üçüncü parti tarafından hizmet alınıyorsa, üçüncü parti tarafından dokümanite edilir.

Bilgi İşlem yöneticisi ve proje yöneticisi değişiklik talebini aşağıdaki konuları da değerlendirerek inceler.

- Program değişikliğine gereksinim ve bu değişikliğin kritikliği
- Mevcut yapıda aynı fonksiyonelliğin elde edileceği yeni yolların araştırılması
- Başka çözümlerin bulunması
- Uygulamanın güvenlik yapısına etkisi
- Diğer modüller / Menü seçenekleri / İş süreci üzerindeki etkisi – Etki Analizi
- Mevcut kontrol prosedürleri üzerindeki muhtemel etkiler
- Değişikliğin gerçekleştirilmesi için gerekli iş yükü

Eğer değişiklik uygulamanın güvenlik yapısını etkiliyorsa, o zaman Bilgi Güvenliği Yöneticisi bu değişikliği analize dâhil eder. Bilgi İşlem yöneticisi ve proje yöneticisi, iş yükünü baz alarak aşağıdaki sınıflandırmaya göre uygulamada yapılacak değişikliğin proje olup olmadığı belirler; 10 adam-gün'den fazla olan değişiklikler proje kapsamında değerlendirilir. Detaylı incelemeden sonra, Bilgi İşlem yöneticisi ve proje yöneticisi görüş ve önerileri mevcutsa analiz dokümanını günceller veya güncellenmesini rica edebilir. Daha sonra değişikliği onaylar.

5.4.3 Onay ve Önceliklendirme

Proje kapsamındaki değişiklikler Bilgi İşlem yöneticisi ve/veya proje yöneticisi, ilgili iş birim yöneticisi ve talebi yapan kişi tarafından onaylanır. Diğer uygulama değişiklikleri Bilgi İşlem yöneticisi ve/veya proje yöneticisi tarafından onaylanır. Yapılan analiz talebi karşılayan Bilgi İşlem personeli tarafından önceliklendirmenin gerçekleştirilebilmesi için gerekli analizler dokümanite edilir. Bu aşamada Bilgi İşlem yöneticisi ve proje yöneticisi tarafından talebin önceliklendirmesine bağlı olarak değişikliğin uygulanması için geliştirme ekibine (şirket içi ekip/ hizmet sağlayıcı) talimatlar verilir.

5.4.4 Değişiklik Yapılması ve Yeni Programların Test Edilmesi

Eğer geliştirme hizmetleri için üçüncü partiden hizmet alınıyorsa, sürüm yönetiminden ve kaynak kodu yönetiminden üçüncü parti sorumludur. Geliştirme şirket içerisinde gerçekleştiriliyorsa, kaynak kodu ve sürüm bakımı Konfigürasyon Yönetimi Prosedürlerine göre yapılır.

Yeni program geliştirildiğinde, bu program birçok testten geçer. Bu testler geliştirme ekibi (şirket içi ekip/ hizmet sağlayıcı) ve uygun test senaryoları ile programların işlevselliğinin

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

testi için iş birimleri tarafından gerçekleştirilir. Ayrıca, test fazında, yeni programların güvenlik açıkları doğurmadığının kontrolü için Bilgi Güvenliği Yöneticisi ve/veya proje yöneticisi da test sürecine dahil edilir. Bu testler sadece test sunucusunda gerçekleştirilir. Canlı ortamında mecbur kalınmadıkça hiçbir test gerçekleştirilemez. Eğer testlerin gerçekleştirilmesi, geliştirilen değişikliğin teknik özelliklerinden dolayı canlı sistemde uygulanmak zorunda ise, bu konuda Bilgi Güvenliği Yöneticisi'ne bilgi iletilir. İş süreci sahipleri ve/veya anahtar kullanıcı test planlarını ve sonuçlarını doğrular.

Tüm test süreci, test planı, prosedürleri ve sonuçlarının detaylı dokümantasyonu ile yedeklenir. Test dokümantasyonu ve sonuçları Bilgi İşlem yöneticisi ve/veya proje yöneticisi tarafından gözden geçirilir ve sonuçlara istinaden değişikliğin uygulanması için onay verilir.

5.4.5 Değişikliğin Uygulanması

Testin başarılı olması üzerine, yeni programlar Bilgi İşlem yöneticisinin ve/veya proje yöneticisinin onayı ile canlı ortama kopyalanır. Programların yalnızca derlenen versiyonları canlı ortama aktarılır. Yeni programlar canlı ortama kopyalanmadan önce veritabanının yedeği alınır. Program değişikliklerinin başarılı bir şekilde tamamlanması için sistem yönetimi ve ilgili iş birimi, ekip oluşturulur.

5.4.6 Değişikliklerin Dokümantasyonu

Geliştirmelerden sorumlu personel, programlardaki değişikliklerin sistem dokümantasyonunu yürütür. Yardım masası üzerindeki değişiklik talepleri için, yapılan değişiklik, değişikliğe ait yardım masası kaydına detaylı bir şekilde yazılır ve değişiklik talebi yardım masası üzerinde kapatılır. Geliştirme ekibi (şirket içi ekip / hizmet sağlayıcı) dışarıdan destek alınan uygulamalar için teknik dokümantasyonu, kullanıcı işletme kitapçığının hazırlanması ve sistem dokümantasyonunun zamanında güncellenmesini sağlar. Yukarıda bahsedilen dokümanları sürdürme sorumluluğu Bilgi İşlem bölümüne aittir.

5.4.7 Acil Durum Program Değişikliği Kontrol Prosedürleri

Yukarıdaki politika ve prosedürlerin dışında kalan, acil aksiyon ve cevap süreci gerektiren tüm program değişiklikleri için şu prosedürler benimsenir:

Geliştirmelerden sorumlu Bilgi İşlem ekibi ilgili iş süreci sahiplerinin sözel ve/veya mail ile onayını alır. Bilgi İşlem yöneticisinin onayı aynı şekilde telefon edilerek veya mail yolu ile alınır.

Geliştirmelerden sorumlu Bilgi İşlem ekibi konunun uzmanları (şirket içi ekip / hizmet sağlayıcı) ile birlikte çalışarak acil program değişikliklerini koordine eder.

Acil durum program değişikliği sırasında normal prosedürler dışında gerçekleştirilen herhangi bir işlem (örn. sorunun çözümü için çalışan destek personeline super-user veya root şifresinin

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

verilmesi) gerçekleştirilmesi durumunda, bunlar belirlenir sistem kabul edilen konfigürasyonuna geri döndürülür.

Acil bir durumda dahi, program değişikliklerini gerçekleştiren destek personeli üzerinde uygun güvenlik kontrolleri uygulanarak, "gerekliliğe göre yetki" prensibi gözetilerek hareket edilir.

Testler, canlı veri ve sistemlerin doğruluk ve bütünlükleri korunarak gerçekleştirilir.

Normal program değişikliği prosedürleri için yapılan dokümantasyonun benzeri acil durum program değişiklikleri için de değişikliğin gerçekleştirilmesinden hemen sonra tamamlanır.

5.4.8 İşletim Sistemi Yamalarının Güncellenmesi

İşletim sistemleri, yetkisiz kişilerin sistemlere erişim için kullanabileceği açıklıkların giderilmesi amacıyla en son çıkan yama ve güncellemelerle güncellenir. Ancak, işletim sistemi yamaları üzerlerinde koşan normal uygulamaları etkileyebilirler. Sistem ve Network Uzmanı şirket içi ekip / hizmet sağlayıcı ile birlikte belirli işletim sistemi yamalarının uygulamanın performans veya güvenliğini etkileyip etkilemediğini kontrol eder. Bilgi Güvenliği Yöneticisi operasyon personelinin yardımıyla uygulama güvenlik kontrollerini, bu kontrollerin doğru ve eksiksiz çalıştığını kontrol etmek için gözden geçirir.

5.4.9 Yazılım Paketlerindeki Değişikliklerin Kısıtlanması

Bir yazılım paketi üzerinde değişiklik yapılması gerektiğinde, aşağıdaki konular değerlendirilir:

- Yerleşik kontrol ve bütünlük süreçlerin zarar görme riski
- Tedarikçinin görüşüne başvurulup vurulmayacağı
- Tedarikçiden gerekli değişikliklerin standart bir program güncellemesi olarak temin edilme olasılığı

Yapılan değişiklikler sonucunda yazılımın daha sonraki bakımından ve idaresinden Şirket'in sorumlu hale gelmesinin doğuracağı sonuçlar.

Değişikliklerin kesin olarak gerekli olması durumunda aşağıdaki adımlar izlenecektir:

Yazılım paketlerinin operasyonel ve güvenlik açısından uygun görülmesi durumunda en son yamalar uygulanır. Eğer en son yama uygulanmayacaksa, bu karar Bilgi İşlem yöneticisi tarafından onaylanmalı ve sebebi dökümanite edilmelidir.

Yamalar önce izole edilmiş bir test ortamında test edilir.

Bu testlerin sonuçları uygulama sahibi tarafından gözden geçirilir ve canlı ortama aktarılmadan önce onaylanır.

Yama / güncellenmenin canlı ortamında uygulanmasından önce bir geri dönüş planı oluşturulur.

Eğer gerçekleştirilecek değişiklik majör bir değişiklik ve Şirket'in operasyonlarını önemli derecede etkileyecek bir geliştirme ise, test sonuçlarının ve program işleyişinin doğrulanması amacıyla bağımsız bir değerlendirme şirketinden hizmet alınması değerlendirilebilir.

Hazırlayan		Onaylayan



Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü

Doküman No	PR.010
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

5.5 Satın Alınan Yazılım Geliştirme Hizmeti

Kullanılacak uygulama üçüncü bir parti tarafından geliştirildiyse, aşağıdaki prosedürler izlenir.

Şirket ve 3. Parti arasında imzalanan anlaşma (Bkz. Tedarikçi Yönetimi Prosedürleri) aşağıdakileri içerir:

- Şirket metodolojisine uygun olarak hazırlanan uygulama geliştirme Yöntemi & Program Değişikliği Kontrol Prosedürleri
- Uygulama kodu, tasarım dokümanları, test planları vb. dokümanların paylaşımı
- Çok acil durumlarda kod değişikliğinin Şirket tarafından gerçekleştirilmesi

Bilgi İşlem Yöneticisi bağımsız bir denetim ve değerlendirme şirketinden, uygulama geliştirme ve bakım prosedürünün tedarikçi ve Şirket arasında yapılan anlaşmaya uygun gerçekleştiğine dair güvence alabilir.

Uygulamaların test edilmesi

Uygulama, bu dokümandaki Uygulama Geliştirme Yöntemi bölümünde verilen test prosedürlerine göre bütünüyle test edilir.

Eğer kaynak koduna erişilebiliyorsa, sistem Trojan koda / gizlenmiş kodlara karşı test edilir.

Sistem yalnızca detaylı testler gerçekleştirildikten sonra kabul edilir ve canlı ortamında uygulanır (Bkz. Sistem planlama ve Kabul Prosedürleri).

Üçüncü taraflar tarafından geliştirilen uygulamalarda herhangi bir değişiklik yapılması gerektiğinde, bu dokümanda Program Değişiklik Kontrolü bölümünde yer alan prosedürler izlenir.

6. İLGİLİ DOKÜMAN

- Sistem Planlama ve Sistem Kabulü Prosedürü
- Bilişim Sistemleri Bakım Onarım Prosedürü

Hazırlayan		Onaylayan