



BURSA ULUDAĞ ÜNİVERSİTESİ

BİDB GÜVENLİ YAZILIM GELİŞTİRME

PROSEDÜRÜ

PR BGYS 011

1. AMAÇ

Bu prosedürün amacı Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığında iç ya da dış kaynakla yapılan uygulama geliştirmelerinin, canlı kullanıma alınmadan önce ve canlı kullanıma alınması esnasında, hangi adımlardan geçmesi gerektiği ile ilgili kuralları belirlemektir.

2. KAPSAM

Bu prosedürde belirtilen ve uyulması gereken hususlar üçüncü taraf firmalara yaptırılan ve Kurum içinde geliştirilen tüm bilgi sistemleri için geçerlidir.

3. TANIMLAR

4. REFERANSLAR

TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Sistemi

TS ISO / IEC 27002 Bilgi Teknolojisi-Güvenlik Teknikleri Bilgi Güvenliği Yönetimi için Uygulama Kuralları

5. UYGULAMA

5.1. Uygulama Geliştirme Taleplerinin Alınması ve Değerlendirilmesi

- Uygulama geliştirme talepleri Bilgi İşlem Daire Başkanlığına UDOS sistemi üzerinden resmi yazı ve FR.3.3.1_01 Yeni Yazılım ve Mevcut Yazılımda Değişiklik Talep formu vasıtasıyla yapılacaktır. Bizzat Yazılım Geliştirme Ekibi tarafından belirlenen uygulama geliştirme ihtiyaçları içinde aynı form kullanılacaktır.
- Talep; ihtiyaç sahibi tarafından söz konusu formun ilgili alanında net ve anlaşılır şekilde açıklanacak ve ilgili birim yöneticisi tarafından mutlaka imzalanacaktır.
- Talep alındıktan sonra Yazılım Geliştirme personeli talebe ilişkin ilgili birimdeki sorumlu personel ile bizzat ihtiyaca ilişkin detaylar üzerinde görüşecek, talebe ilişkin değerlendirmesi ile birlikte Genel Müdür onayını alacaktır.
- Talebe ilişkin işlemler tamamlandıktan sonra ihtiyaç sahibi birim yöneticisinin ihtiyacın karşılandığına dair onayı alınarak form ilgili klasörde muhafaza edilecektir

5.2. Uygulama Geliştiricinin Seçimi

Onay sonrası iş listesine alınan uygulama geliştirme ihtiyacının BT Personeli tarafından mı yoksa tedarikçi tarafından mı yapılacağına Daire Başkanı karar verilir. Bu kararın verilmesinde aşağıdaki kısıtlar dikkate alınır;

- Yapılacak geliştirmenin niteliğinin uygulamanın bütünlüğünü, entegre yapısını tehlikeye düşürecek nitelikte olup olmaması,
- Geliştirme talep edilen uygulama üzerinde sözleşme gereği uygulamanın bütünlüğünü bozacak geliştirmelerin yalnızca yetkili tedarikçiler tarafından yapılabileceği,
- Mevcut Geliştirme personelinin bilgi ve tecrübesi,
- Geliştirme Personelinin iş yoğunluğu.

Eğer geliştirme dış kaynak kullanılarak yapılacaksa.

- Olası tedarikçilere iletilecek talep netleştirilir,
- Geliştirmeyi yapabilecek tedarikçiler referansları, uzmanlık konuları ve piyasa imajları göz önüne alınarak filtreleme sonrası görüşmelere çağırılır,
- İşin birlikte yapılmasına karar verilen tedarikçilere, gizlilik sözleşmesi imzalatılır,
- Seçilen tedarikçiden varsa sözleşme istenir, sözleşme yoksa Yazılım Geliştirme Ekibi tarafından hazırlanır ve Hukuk Departmanına gönderilir. Gelen yorumlar doğrultusunda gerekli düzeltmeler yapıldıktan sonra sözleşme taraflarca imzalanır,
- Tedarikçi, geliştirmeyi talep eden departman ve Yazılım Geliştirme Ekibi, kaynakları gözden geçirerek proje planını hazırlar.
- İşin beraber yapılacağı ekip üyeleri belirlenir.
- Geliştirme talep eden iş birimi, talepte bulunduğu süreçle ilgili detaylı bilgileri ve iş akış şemalarını sağlar,
- Tedarikçi, Yazılım Geliştirme ekibi ve iş birimiyle gerekli görüşmeleri yaparak analiz dokümanını oluşturur,
- Analiz dokümanı iş birimine onaylatılır,
- Tedarikçi, analiz dokümanına istinaden iş planını yapar ve geliştirme faaliyetlerine başlar.

Eğer geliştirme BT Departmanı tarafından yapılacaksa;

- İşin yazılım personeli belirlenir.
- Yazılımcı ihtiyaç sahibi birim ile görüşerek detay konuları belirler ve kaynakları gözden geçirerek proje planını hazırlar,
- Geliştirme talep eden iş birimi, talepte bulunduğu süreçle ilgili detaylı bilgileri ve iş akış şemalarını sağlar,
- Yazılım Geliştirme Ekibi, ilgili iş birimiyle gerekli görüşmeleri yaparak analiz dokümanını oluşturur,
- Analiz dokümanı iş birimine onaylatılır,
- Yazılımcı, analiz dokümanına istinaden iş planını yapar ve geliştirme faaliyetlerine başlar

5.3. Uygulamanın Geliştirilmesi

Geliştirme:

- İş için yapılan yazılım geliştirmeleri “Geliştirme (Development) Ortamları” nda yapılır;
- Yazılım sırasında giriş verisinin geçerlemesi ve kullanıcıların yanlış veri girmemesi amacı ile gerekli kontroller uygulanır.
- Performans sıkıntısı oluşabilecek uygulamalar için stres testleri yapılır,
- Veri tabanı tarafında obje isimlendirmesi yapılırken standartlara uyulur. Oluşturulan objeler için Veri Tabanı Yöneticisi tarafından bir sahiplik belirlenir ve obje isimlerinin başına bu sahiplik eklenir.

Test Ortamı:

- Yazılımcı testleri bitirildikten sonra geliştirmeler “TEST” ortamına aktarılır. “TEST” ortamında yapılan işin analiz dokümanına uygunluğu gözden geçirilir. Girilen test bilgileri,

kurallara uygunluğu ve bütünlüğü açısından yazılımcı tarafından eldeki örnek veriler ile kontrol edilir.

- Test senaryoları anahtar kullanıcılar tarafından hazırlanır ve iş birimi testlerini bu senaryolar kapsamında “TEST” ortamında gerçekleştirir ve test sonuçlarını yazılım ekibine bildirir.
- İş geliştirme sırasında ya da test sonuçları içinde, onaylanmış analiz dokümanında yer almayan herhangi bir değişiklik/yeni bir iş talebinin yeniden değerlendirme ve onay sürecinden geçmesi gerekir,
- Talep onaylanırsa iş planı revize edilir, yazılım sürecine geri dönülür.

Canlı Ortam Geçişi ve İş Kapama:

- Canlı kullanıma geçiş planına uygun olarak projeyi talep eden departman çalışanları (key user) tarafından eğitimler verilir ve doküman hazırlanır.
- Canlı kullanım desteğinin nasıl yapılacağı planlanır.
- “TEST” ortamında onaylanan geliştirme “LIVE” sisteme alınır.
- Canlı kullanıma geçiş yapılır ve bu ortamda yeni yapılan geliştirmelerin sağlıklı çalışıp çalışmadığı ile ilgili iş birimi tarafından yazılım ekibine geri bildirim yapılır.
- Uygulama devreye alınıp canlı kullanımda sağlıklı kullanımı onaylandığında, mevcut sistemin sürekliliğini sağlamak adına gerekli kontroller yapılır.
- Yapılan geliştirmenin iş birimi tarafından “LIVE” sistemde onaylanmasının ardından iş kapanışı yapılır.

Dikkat Edilmesi Gerekenler:

- Uygulama Geliştirmelerin, canlı kullanıma alınmasının ardından projede yer alan tedarikçinin destek faaliyetlerini farklı bir şirkete devretmesi gibi durumlarda görevi devralan şirketten gizlilik sözleşmesi talep edilir. Bu tip devirler tercih edilmemekle beraber sadece uygulama desteği açısından ve sadece canlı kullanıma geçiş sonrasında hatasız çalışan bir uygulama için gerçekleştirilir.
- Dış tedarikçiler tarafından yapılan uygulama geliştirme faaliyetlerinde kapsamında kişilerin kimlik bilgileri talep edilir. Söz konusu kişilerin çalışmalarını yürütmeleri için belirlenen sunucu ya da sistemlere erişimi gerekiyorsa söz konusu kişiler adına hesap açılarak yapacakları çalışmaları bu hesaplarla yapmaları sağlanır. Söz konusu hesaplarla yapılacak uzaktan erişimlerin yalnızca yetkili kılındıkları sunuculara yapılması sağlanır. Tedarikçi ile yapılacak sözleşmelere geliştirme yapan yazılımcıların işten ayrılmalarında zaman kaybetmeksizin şirketimize bildirmeleri özel bir madde olarak eklenir.
- Uygulama geliştirme kodların şirket dışına çıkarılmaması ve 3. şahıslara izinsiz olarak gösterilmemesi için çalışanlara “Gizlilik Sözleşmesi” imzalatılarak gerekli önlemler alınır. Ayrıca bu taahhütname ile uygulama süresince tüm satın alınan yazılımlar ve yazılımlara ait araçların kullanım hakları şirketimize ait olup, dışarı çıkarılmaması ve 3. şahıslara izinsiz verilmemesi sağlanır, aksi durumlarda disiplin süreci işletilir.

6. SORUMLULUK

Bilgi İşlem Departmanı ya da dış taraflarca yapılacak uygulama geliştirme faaliyetlerinde burada anlatılanları uygulamaktan Yazılım Geliştirme personeli sorumludur. Ayrıca uygulama geliştirme talep eden birim aşağıdakileri yapmaktan sorumludur;

- Geliştirme talebinde bulunduğu süreçle ilgili detaylı bilgileri ve iş akış şemalarını sağlamaktan,
- Geliştirme sürecinde yer alacak fonksiyonel kaynakları tedarik etmekten,



BURSA ULUDAĞ ÜNİVERSİTESİ
BİDB GÜVENLİ YAZILIM GELİŞTİRME
PROSEDÜRÜ

PR BGYS 011

- Canlı kullanıma geçiş öncesinde geliştirilen uygulamayı, departmanın hazırladığı senaryoya göre test etmekten,
- Geliştirilen uygulamanın, canlı kullanıma alınması için uygunluk onayını vermekten,
- Canlı kullanıma geçiş sonrası, uygulamaya dair geri bildirim yapmaktan.

7. KONTROL

Dokümanlar ihtiyaç halinde revize edildiği gibi, yılda bir kez periyodik olarak kontrol edilir.

8. EKLER