İÇİNDEKİLER

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

1 AMAÇ

Bu prosedürün amacı EGE Üniversitesi Hastanesi (Sağlık Uygulama ve Araştırma Merkezi) Bilgi İşlem Birimi bünyesinde gerçekleştirilen yazılım geliştirme ve destek süreçlerinde bilgi güvenliğinin sağlanmasıdır.

2 KAPSAM

EGE Üniversitesi Hastanesi (Sağlık Uygulama ve Araştırma Merkezi) Bilgi İşlem Birimi bünyesinde faaliyet gösteren Yazılım Grubu faaliyetleri bu prosedür kapsamındadır.

3 TANIMLAR VE KISALTMALAR

YGG: Yönetim Gözden Geçirme
BİB: Bilgi İşlem Birimi
EGE ÜNİ. HST.: EGE Üniversitesi Hastanesi
BGYS: Bilgi Güvenliği Yönetim Sistemi

4 SORUMLULAR

Bu prosedürün oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Bu süreçte BGYS Yönetim Temsilcisine Yazılım Grubu tarafından destek verilir.
Prosedürün uygulanmasından Yazılım Grubu sorumludur.

5 UYGULAMA

5.1 GENEL GELİŞTİRME POLİTİKASI

- Yazılım geliştirme süreçleri fiziksel olarak kontrollü bir ortamda yapılır.
- Proje yönetim süreçlerinde; iş önceliği Bilgi İşlem Daire Başkanlığı tarafında verilir. Yazılım ekibi ufak olduğu için yazılım projeleri yazılım ekibi arasında paylaşımlı ve yedekli olarak yürütülür.

- Yazılım geliştirme işlemlerinde görev atamalarında, e-posta sistemi ve EBYS uygulaması kullanılır.
- Güvenli yazılım geliştirme konusunda farkındalığı yüksek bir personel grubuyla çalışılmaktadır.

5.2 YAZILIM GELİŞTİRME ADIMLARI

5.2.1 Müşteri Gereksinimlerinin Çıkarılması

- Müşteri gereksinimleri yazılım uzmanları tarafından sahada yapılan gözlemlerden ve müşterilerden gelen taleplerden çıkarılır. Yeni bir yazılım üretimi için e-posta üzerinden ilgili taraflardan talep alınır.
- Sahada olan ürünler için talepler EGE ÜNİ. HST. İş Takip Sistemi üzerinden alınır.
- Anlaşılamayan müşteri talepleri için müşteriyle EGE ÜNİ. HST. İş Takip Sistemi üzerinden yazışmalar yapılır.

5.2.2 Yazılım Gereksinimlerinin Çıkarılması ve Tasarım

Müşteri talepleri analiz edilerek Yazılım gereksinimleri çıkarılır. Veritabanı, arayüz tasarımları yapılır. Elde edilen bu bilgilere dayanarak, yazılım uzmanı tarafından yazılım geliştirilmeye başlanır.

5.2.3 Kodlama ve Entegrasyon

Yazılım gereksinimlerine ve yapılan tasarımlara uygun olarak yazılım birimlerinin kodlanması ve entegrasyonu gerçekleşir. Konfigürasyon yönetim aracı olarak SVN kullanılmaktadır. Kod kalitesi ve güvenliği taraması için karşılıklı kod review süreçleri işletilir.

5.2.4 Testler

Ortaya konan yazılım ürünü sahaya çıkmadan önce testlere tabi tutulur. Test işlemleri ile ürünün yazılım gereksinimlerini sağlama durumu kontrol edilir.
Test işlemleri, geliştirme işlemini yapan yazılım personelinden başka bir personel tarafından gerçekleştirilir.

Test işlemleri yapılırken operasyonel veriler kullanılmaz.

5.2.5 Sürüm Yayınlama

Test işleminden geçmiş yazılım ürünü için sürüm yayınlama yapılır. Sürüm yayınlanmadan önce hazırlanmış sürüm paketi yazılım gurubu sorumlusu veya başka bir yazılım geliştirme sorumlusu tarafından kontrol edilir.
Kodlar operasyonel ortama atılmadan önce Konfigürasyon Yönetim Ortamında hazır bulunur.

5.3 GÜVENLİ YAZILIM GELİŞTİRME PRENSİPLERİ

- Veri tabanı bağlantılarında SSL türü güvenli bağlantı yöntemleri tercih edilmelidir.
- Veri tabanı için oluşturulan kullanıcı yetkileri sadece ilgili uygulamaya ait veri tabanına erişecek şekilde yapılandırılmalıdır.
- Veri tabanında gizli bilgilerin açık ve okunabilir bir şekilde tutulması engellenmelidir.
- Yazılımlarda kod geliştirme esnasında erişim kısıtlamaları doğru ve kontrollü bir şekilde uygulanmalıdır.
- Aykırı durumların (exceptions) bir sistem hakkında gizli ve fazla bilgiler vermesine engel olacak hatalar üretilmelidir. (örn: “şifreniz hatalı” yerine “kullanıcı adı veya şifre hatalı”)
- İzin tanımlamasında “en düşük erişim hakkı” prensibi uygulanmalıdır.
- Güvenilir olmayan kodların kritik metotları kullanılmamalıdır.
- XSS (Cross-Site Scripting) ve SQL injection gibi OWASP tehdidi yüksek saldırılara karşı önlem alınmış kodlar yazılmalıdır.
- Web uygulamalarında SSL teknolojileri kullanılmalıdır.
- Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının net olarak tanımlanması sağlanmalıdır.
- Periyodik olarak yetki kontrollerinin gerçekleştirilmesi yapılmalıdır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması sağlanmalıdır. Gerekirse yazılım ve veritabanı şifrelerinin de değiştirilmesi sağlanmalıdır. Bu kapsamda, kendisine tahsis edilen envanterin iade alınması sağlanmalıdır.

- Özel nitelikli verilerin korunmasında, muhafaza edildiği ve/veya erişildiği ortamlar için aşağıdaki koşulların sağlanması gerekmektedir:
- Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
- Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,

5.4 GELİŞTİRME ORTAM GÜVENLİĞİ

- Yazılım geliştirme işlemi fiziksel olarak korunaklı ve sadece yetkili personelin erişebileceği ortamlarda gerçekleştir.
- Yazılım kaynak kodlarına sadece ilgili yazılım erişim geliştirme uzmanlarının erişimi vardır.
- Test, geliştirme ve operasyonel ortam birbirinden ayrılmıştır.
- Yazılım kaynak kodları SVN ortamından yedeklenir.
- Kodlarda yapılan değişikler SVN aracı ile gözlemlenir.

5.5 DIŞ KAYNAK KULLANIMI

Yazılım geliştirme süreçlerinde dış kaynak kullanımı yapılmamaktadır.

5.6 GÜVENLİK KABUL VE TEST FAALİYETLERİ

Yazılım geliştirme işlemleri gerçekleştirdikten sonra, uzman personel tarafından otomatik güvenlik tarama araçları veya code review süreçleri kullanılarak güvenlik kontrolleri yapılır.

6 İLGİLİ DOKÜMANLAR

İlgili doküman bulunmamaktadır.