1. AMAÇ

İYTE Bilgi İşlem Daire Başkanlığı içerisinde geliştirilen yazılımların temel yöntemlerini belirlemek amacıyla yazılmıştır.

2. KAPSAM

İYTE Bilgi İşlem Daire Başkanlığı içerisinde geliştirilen yazılımlardır.

3. KISALTMALAR VE TANIMLAR

Terim	Tanım/Açıklama
BGYS	Bilgi Güvenliği Yönetim Sistemi
Kurum	**İYTE Bilgi İşlem Daire Başkanlığı**

4. GÜVENLİ YAZILIM GELİŞTİRME POLİTİKASI

4.1. Yazılım Geliştirme

Kurum'da ihtiyaç duyulan yazılımlar Daire Başkanı'na iletilir. Talep doğrultusunda Yönetim ve ilgili birimlerle toplantılar gerçekleştirilir. Yazılım projesinin tüm detayları netleştirilir. Yazılım projesi için Daire Başkanı sorumlu bir personel belirler. Projenin kapsamına bu iş için bir ekipte kurulabilir. Talep sahibi birimlerden proje detayları hakkında destek almak üzere personel belirlenmesi istenir.

Analiz, tasarım, geliştirme, test ve işletim ortamları, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmaktadır. Bu ortamların tamamı birimimizde görev yapan "Yazılım Ekibi" tarafından gerçekleştirilmektedir. Proje geliştirmenin tüm aşamalarında "Analiz" bölümünde hazırlanan "Proje Planları"na uyulmasına özen gösterilir.

Analiz, tasarım, geliştirme, test ve işletim ortamlarında gerçekleştirilen işlemler sırasıyla aşağıda verilmektedir:

4.1.1. Analiz

(1) Talep edilen yazılımın tüm detayları netleştirilir. Yazılım projesi için Daire Başkanı tarafından ''Yazılım Ekibi'' belirlenir.

(2) Talep edilen yazılımın donanım ve sistem gereksinimleri tespit edilir.

(3) Yazılımın özellikleri ve yazılım personelinin teknik yeterlilikleri doğrultusunda Programlama diline karar verilir.

(4) Veri tabanı yapısı ve kimlik doğrulama yöntemleri belirlenir.

(5) Proje ekibinin ilgili sunuculara ve servislere erişim yetkileri düzenlenir.

(6) İhtiyaç duyulan/kullanılacak web servisler belirlenir. Verinin kaynağına göre iç ve dış paydaşlarla resmi kanallarla iletişim kurulur ve talep edilen veriler bildirilir.

(7) Yazılım tasarımının (web sayfası, yönetim ve kullanıcı ara yüzleri vs.) geliştirme metoduna karar verilir.

(8) Proje ekibi/destek personeli ve personelin hastalık, izin ve vekalet durumları göz önünde bulundurularak insan kaynakları planlaması yapılır.

(9) Yukarıda belirtilen tüm detaylar netleştirildikten sonra proje yöneticisi tarafından proje planı oluşturulur.

4.1.2. Tasarım

1) Analiz aşaması tamamlanan projenin belirlenen gereksinimleri doğrultusunda yazılımın temel yapısı oluşturulur.

2) Yazılımın görsel tasarımı yapılır.

4.1.3. Geliştirme

1) Ortaya koyulan veriler doğrultusunda yazılımın gerçekleştirildiği aşamadır.

2) Analiz kısmında karar verilen yapıya göre veri tabanı oluşturulur.

3) Kodlama çalışmaları yapılır.

4) Kullanılan kütüphaneler vb. yazılım paketlerinde değişiklik yapılması gerektiğinde önce yedek alınmalı sonra ilgili değişiklik yapılmalıdır.

5) Jıra, bıt backer üzerinde kodların versiyonları tutuluyor, bambu üzerinden kullanıcılara dıploy yapılıyor.

4.1.4. Test

1) Test aşaması, kodlama sürecinin ardından gerçekleştirilen sınama ve doğrulama aşamasıdır.

2) Elde edilen uygulama yazılımının hem belirlenen gereksinimleri sağlayıp sağlamadığı hem de gerçekleştirimin beklentilere uygun olup olmadığını kontrol etmek için statik ve dinamik sınama tekniklerinden yararlanılır.

3) Hazırlanan yazılımın ilk test aşaması proje ekibi tarafından lokal ortamda gerçekleştirilir.

4) Tespit edilen eksiklikler giderildikten sonra sunucuya aktarım işlemi yapılır. Uygulama, İş takvimine göre önceden belirlenmiş zaman aralığında yetkilendirmelerle sınırlandırılarak pilot bir bölgede kullanıma açılır. Pilot bölgenin kullanıcılarına bilgilendirme yapılır ve uygulamayla ilgili geri bildirimler toplanır. Bu şekilde hazırlanan yazılımın ikinci test aşaması tamamlanır. Geri bildirimlere göre eksiklikler tespit edilerek giderilir.

5) Test ortamında kullanılacak veriler içerisinde kişisel bilgiler bulundurulmaz yada anonimize edilir.

4.1.5. İletişim

1) Test aşamaları tamamlanan yazılım son kullanıcı seviyesinde kullanıma açılır.
2) Uygulama; Yönetim ve son kullanıcılardan gelen taleplere göre belirli periyotlarla geliştirilmeye devam edilir.
3) İşletim platformunda değişiklik yapılması gerektiğinde tüm süreç yazılım geliştirme ekibi tarafından yürütülür.

4.2. Güvenlik

Yazılım geliştirmenin tüm aşamalarında aşağıda belirtilen güvenlik maddeleri uygulanmalıdır:

1) Uygulamaların kayıt altına aldığı veya kullandığı her türlü bilginin yetkisiz erişime kapalı olması gerekmektedir.
2) Web, uygulama ve veritabanı sunucularının sistem bileşenleri hakkındaki kritik bilgileri (sunucu adı ve sürümü, kullanılan program sürümü vb.) gizlenmelidir.
3) Veritabanı, uygulama sunucusu ve web sunucusu gibi kullanılan yazılımların güvenlik yamaları en üst seviyede olmalıdır.
4) Kullanılan parolalar ve parolamı unuttum kontrol soru ve cevapları gibi diğer hassas veriler açık metin olarak saklanmamalıdır.
5) Uygulamalar, geliştirme ortamından test ortamına aktarılırken gereksiz olan dosyalar (örneğin test kodlar, demo programlar, yedek dosyalar) silinmeli, gerek yoksa kaynak kod aktarılmamalı ve aktarılacak olan kaynak kodlardaki yorum satırları silinmelidir. Aktarım esnasında dosyalarda istenmeyen bir değişikliğin olmaması garanti edilmelidir.
6) Uygulamada oluşan hatalar ve uygulama sunucusu ön tanımlı hata mesajları kullanıcıya detaylı olarak gösterilmemelidir.
7) Uygulamaların üzerinde bulunduğu sunucular, servis verdikleri dizinlerin içeriklerini listelememelidir.
8) Ana sistem için gereksiz olan dosyalara (örneğin yedekleme, arşiv, test, geliştirme için kullanılan dosyalar) erişim engellenmeli ve sistemdeki gereksiz uygulamalar (örneğin ön tanımlı sunucu sayfaları, demo uygulamalar) kaldırılmalıdır.
9) GET ve POST isteklerindeki HTTP parametreleri değiştirilerek üçüncü şahısların bilgilerine yetkisiz olarak erişilmemelidir.
10) Uygulamayı çalıştıran sistem kullanıcısının, hizmet verilen dizin dışındaki yetkileri kaldırılmalıdır.
11) Veritabanı kullanıcısının sadece uygulamanın kullandığı veritabanı kaynaklarına erişim hakkı olmalıdır.
12) Sunucu üzerinde bulunan ve web tabanlı istatistik sağlayan uygulamalara erişim herkese açık olmamalıdır.

13) Kısıtlı erişim gerektiren bütün URL'lere, servislere, uygulama verilerine, kullanıcı bilgilerine, güvenlik yapılandırma dosyalarına erişim denetlenmelidir.

14) Yetki hakkının artık gerekmediği durumlarda (örneğin kurumdan ayrılma, projede rol değiştirme gibi) en kısa sürede ilgili haklar iptal edilmelidir.

15) Yönetim paneli gibi kritik dizinlerin isimleri kolay tahmin edilebilir olmamalıdır (admin, yönetici, administrator).

16) Erişime açılan her kaynak kimlik denetimine tabi tutulma yöntemini de kullanmak zorundadır.

17) Umumi olmayan bütün kaynaklara ve sayfalara erişim için sunucu tarafında kimlik doğrulaması yapılmalıdır.

18) Kullanıcı adı ve parola ile kimlik doğrulamasının yapıldığı kontroller tek tip hata mesajı vermek suretiyle kullanıcı adları listeleme saldırılarına engel olmalıdırlar. Örnek bir hata mesajı "Girdiğiniz kullanıcı adı ve/veya parola yanlıştır." seklinde olabilir.

19) Bütün başarılı ve başarısız login işlemleri ve kaynaklara erişim denemeleri kayıt altına alınmalıdır.

20) Oturum bilgisi zaman aşımına uğrayacak şekilde yapılandırılmalıdır.

21) Dış taraflardan kritik uygulama sağlanması gerektiğinde, kurumsal standartlar ve güvenlik prensiplerine uygun şekilde çalışılmalıdır.

22) Tüm sistemler geliştirme yaşam döngüsü boyunca güvenli geliştirme ortamında sürdürülür.

23) Geliştirilen sistemlerde güvenlik testleri yapılmalıdır.

5. İLGİLİ DOKÜMANLAR

5.1. İç Kaynaklı Dokümanlar

5.2. Dış Kaynaklı Dokümanlar

TS ISO/IEC 27001:2022 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler