

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	YAZILIM GELİŞTİRME ve TEMİN PROSEDÜRÜ	Doküman No	BGYS-PR26
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	09.07.2024
		Revizyon No	03
		Sayfa No	1 / 10

1. AMAÇ

Bu prosedür, birimimiz tarafından geliştirilen yazılım süreçlerini belirlemek için oluşturulmuştur.

2. KAPSAM

Bu prosedür, Bilgi İşlem Dairesi Başkanlığı bünyesinde görev yapan tüm personel ve yüklenicileri kapsar.

3. SORUMLULUK

Bu prosedürün işletilmesinden Yazılım Hizmetleri Şube Müdürü sorumludur.

4. TANIMLAR VE KISALTMALAR

BİDB	: Bilgi İşlem Dairesi Başkanlığı
Birim	: Genel Müdürlük ya da Daire Başkanlığı
Uygulama	: Yazılım
Kurum	: Gençlik ve Spor Bakanlığı

5. YAZILIM GELİŞTİRME

5.1. Yazılım Talebi

Yazılım ihtiyacı olan birim, BİDB'den toplantı talep eder, yapılan toplantılar sonucunda onaylanan yazılım projesinin detayları netleştirilir ve toplantı karar tutanağı doğrultusunda çalışmalar başlatılır. Yazılım Şube Müdürü sorumlu bir personel veya ekip belirler. Talep sahibi birimlerden proje detayları hakkında destek almak için 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 planlarına uyulmasına özen gösterilir.

5.2. Analiz

Analiz ekibi yazılım talebinde bulunan birim ile görüşüp yazılım ihtiyaçlarını belirler ve gerekli analiz raporunu oluşturur.

- Talep edilen yazılımın tüm detayları netleştirilir. Yazılım projesi için Yazılım Şube Müdürü tarafından Yazılım Ekibi belirlenir.
- Talep edilen yazılımın donanım ve sistem gereksinimleri tespit edilir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	YAZILIM GELİŞTİRME ve TEMİN PROSEDÜRÜ	Doküman No	BGYS-PR26
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	09.07.2024
		Revizyon No	03
		Sayfa No	2 / 10

- Yazılımın özellikleri ve yazılım personelinin teknik yeterlilikleri doğrultusunda programlama diline karar verilir.
- Veri tabanı yapısı ve kimlik doğrulama yöntemleri belirlenir.
- Proje ekibinin ilgili sunuculara ve servislere erişim yetkileri düzenlenir.
- İhtiyaç duyulan/kullanılacak web servisler belirlenir. Verinin kaynağına göre iç ve dış paydaşlarla resmi kanallar yoluyla iletişim kurulur ve talep edilen veriler karşılıklı olarak bildirilir.
- Yazılım tasarımının (web sayfası, yönetim ve kullanıcı ara yüzleri vs.) geliştirme metoduna karar verilir.
- Proje ekibi/destek personeli ve diğer personelin hastalık, izin ve vekâlet durumları göz önünde bulundurularak insan kaynakları planlaması yapılır.

5.3. Tasarım

- Analiz aşaması tamamlanan projenin belirlenen gereksinimleri doğrultusunda yazılımın temel yapısı oluşturulur.
- Yazılımın görsel tasarımı yapılır. Yazılımın kapsamına göre ilgili birim tarafından görsel tasarımın da yapılması istenebilir.
- Tasarım sürecinde güvenlik gereksinimleri tanımlanmalı ve bu gereksinimler göz önünde bulundurularak tasarım yapılmalıdır. Tedarik edilen veya hizmet alımı ile geliştirilen uygulamaların teknik şartnamelerinde güvenlik gereksinimlerine yer verilmelidir.
- Uygulamalar, tüm oluşabilecek hataları yakalayabilecek ve hata durumlarında varsayılan olarak güvenli durumlara geçecek şekilde tasarlanmış olmalıdır. Örneğin, yetkilendirme esnasında hata oluşması durumunda uygulama ilgili işlemi durdurmalı ve kullanıcı yetkilendirilmemelidir. Kimlik doğrulama işlemi sırasında hata ile karşılaşıldığında ise kullanıcının uygulamaya girişi engellenmelidir. Hata durumu ile ilgili detaylar kullanıcıya gösterilmemelidir.
- Uygulamanın entegre olunan sisteme ulaşamaması veya sistemin hata dönmesi durumlarında, uygulama kararlı ve güvenli şekilde işlemlerini devam ettirebilecek şekilde tasarlanmalıdır. Uygulama bu durumlarda hizmet sürekliliğini sağlayacak fonksiyonlara sahip olmalıdır.
- Veri tabanı tasarımı kişisel verilerin yedekleme, anonimleştirme ve veri aktarımı işlemlerini kolaylaştıracak şekilde yapılmalıdır.

5.4. Geliştirme

Ortaya koyulan veriler doğrultusunda yazılımın gerçekleştirildiği aşamadır.

- Analiz kısmında karar verilen yapıya göre veri tabanı oluşturulur.
- Kodlama çalışmaları yapılır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	YAZILIM GELİŞTİRME ve TEMİN PROSEDÜRÜ	Doküman No	BGYS-PR26
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	09.07.2024
		Revizyon No	03
		Sayfa No	3 / 10

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

5.5. Veri tabanı Oluşturulması ve Veri tabanı Erişim Yetkilendirilmesinin Belirlenmesi

Analiz sürecinde ihtiyaçları belirlenen yazılımın veri tabanının oluşturulması ve bu veri tabanı üzerinde çalışacak kişilerin yetkilerinin belirlenmesi veri tabanı ekibi tarafından yapılır.

5.6. Kodlama

Yazılım Geliştirme ekibi kodlama sürecini gerçekleştirir.

5.6.1 Planlama ve Kodlama Öncesi

Güvenli kodlama ilkeleri hem yeni geliştirmelerde hem de yeniden kullanım senaryolarında kullanılmalıdır. Bu ilkeler, hem kuruluş içindeki geliştirme faaliyetlerine hem de kuruluş tarafından başkalarına sağlanan ürün ve hizmetlere uygulanmalıdır. Kodlamadan önceki planlama ve ön koşullar aşağıdakileri içermelidir:

- Hem kurum içi hem de dış kaynaklı kod geliştirmelerinde kullanılacak güvenli kodlama için kuruluşa özgü beklentileri ve onaylanmış ilkeleri,
- Bilgi güvenliği açıklarına yol açan yaygın ve tarihsel kodlama uygulamaları ve kusurları,
- Güvenli kod oluşturulmasını zorlamaya yardımcı olmak için tümleşik geliştirme ortamları (IDE) gibi geliştirme araçlarının yapılandırılması,
- Uygunsa, geliştirme araçları ve yürütme ortamları sağlayıcıları tarafından yayımlanan kılavuza uyulması,
- Güncellenmiş geliştirme araçlarının (örneğin, derleyiciler) bakımı ve kullanımı,
- Geliştiricilerin güvenli kod yazma konusundaki nitelikleri,
- Tehdit modelleme dahil olmak üzere güvenli tasarım ve mimari,
- Güvenli kodlama standartları ve ilgili olduğu durumlarda bunların kullanımının zorunlu kılınması,
- Geliştirme için kontrollü ortamların kullanımı.

5.6.2 Kodlama Sırasında

Kodlama sırasında dikkate alınması gereken hususlar aşağıdakileri içermelidir:

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	YAZILIM GELİŞTİRME ve TEMİN PROSEDÜRÜ	Doküman No	BGYS-PR26
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	09.07.2024
		Revizyon No	03
		Sayfa No	4 / 10

- a) Kullanılan programlama dillerine ve tekniklerine özgü güvenli kodlama uygulamalarını,
- b) İkili programlama, yeniden düzenleme, akran incelemesi, güvenlik yinelemeleri ve test güdümlü geliştirme gibi güvenli programlama tekniklerinin kullanılmasını,
- c) Yapılandırılmış programlama tekniklerinin kullanılmasını,
- d) Bilgi güvenliği açıklarının kullanılmasına izin verebilecek kodun dokümente edilmesi ve programlama kusurlarının ortadan kaldırılmasını,
- e) Güvenli olmayan tasarım tekniklerinin kullanımının yasaklanmasını (örneğin; sabit kodlanmış parolaların, onaylanmamış kod örneklerinin ve kimliği doğrulanmamış web hizmetlerinin kullanımı). Test, geliştirme sırasında ve sonrasında yapılmalıdır. Statik uygulama güvenlik testi (SAST) süreçleri, yazılımdaki güvenlik açıklarını belirleyebilir. Yazılım çalışır hale getirilmeden önce aşağıdakiler değerlendirilmelidir:

- a) Saldırı yüzeyi ve en az ayrıcalık ilkesi,
- b) En yaygın programlama hatalarının analizinin yapılması ve bunların hafifletildiğinin belgelenmesi.

5.6.3 İnceleme ve Bakım

Kod çalışır hale getirildikten sonra:

- a) Güncellemeler güvenli bir şekilde paketlenmeli ve dağıtılmalıdır,
- b) Bildirilen bilgi güvenliği açıkları ele alınmalıdır,
- c) Hatalar ve şüpheli saldırılar günlüğe kaydedilmeli (logları tutulmalı) ve loglar düzenli olarak gözden geçirilerek kodda gerektiği gibi ayarlamalar yapılmalıdır,
- d) Kaynak kodu, yetkisiz erişime ve kurcalamaya karşı korunmalıdır (örneğin, tipik olarak erişim kontrolü ve sürüm kontrolü gibi özellikler sağlayan yapılandırma yönetimi araçları kullanarak). Harici araçlar ve kütüphaneler kullanılıyorsa kuruluş aşağıdakileri dikkate almalıdır:

- a) Harici kütüphanelerin yönetilmesini (örneğin, kullanılan kütüphanelerin ve sürümlerinin bir envanterini tutarak) ve yayın döngüleriyle düzenli olarak güncellenmesinin sağlanmasını,
- b) İyice incelenmiş bileşenlerin, özellikle kimlik kanıtlama ve kriptografik bileşenlerin seçimi, yetkilendirilmesi ve yeniden kullanımı,
- c) Harici bileşenlerin lisansı, güvenliği ve geçmişi,

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	YAZILIM GELİŞTİRME ve TEMİN PROSEDÜRÜ	Doküman No	BGYS-PR26
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	09.07.2024
		Revizyon No	03
		Sayfa No	5 / 10

d) Yazılımın bakımının yapılabilir olmasının, izlenebilir ve kanıtlanmış, saygın kaynaklardan geldiğinin sağlanması,

e) Geliştirme kaynaklarının ve eserlerinin yeterince uzun vadeli mevcudiyeti.

Bir yazılım paketinin değiştirilmesi gerektiğinde aşağıdaki noktalar dikkate alınmalıdır:

a) Yerleşik kontrollerin ve bütünlük süreçlerinin tehlikeye girme riski,

b) Tedarikçinin onayını alıp almamak,

c) Standart program güncellemeleri olarak tedarikçiden gerekli değişiklikleri elde etme ihtimali,

d) Kuruluşun, değişikliklerin bir sonucu olarak yazılımın gelecekteki bakımından sorumlu olması durumundaki etkisi,

e) Kullanılan diğer yazılımlarla uyumluluk.

5.6.4 Program Kaynak Koduna Erişim Kontrolü

Program kaynak kodunun ve kütüphanelerinin alınması ve saklanması ile ilgili hususlar, yazılım temin yoluyla alındıysa şartnamelerde belirtilir. Kaynak koduna erişimlerin kısıtlanması için en az aşağıdaki adımlar göz önünde bulundurulur.

- Kaynak kod ve kütüphaneler, canlı uygulama ortamında tutulmaz.
- Personelin kaynak kod ve kütüphanelerine erişimi, ihtiyaçlara göre sınırlandırılır.
- Program kaynak kod ve kütüphanesine erişimler ilgili birim amirinin bilgisi dahilinde yapılır.
- Program kaynak kod ve kütüphanesi ile ilgili değişiklikler için olay kayıtları tutulur ve saklanır.
- Değişiklikler öncesi kaynak kod ve kütüphanelerinin tüm sürümleri saklanır.
- Geliştirme ortamı, test ortamı ve canlı ortamın kaynak kodları farklı ortamlarda olmalıdır.
- Yalnızca onaylı yazılım kütüphanelerinin (* .dll, * .ocx, * .so vb.) yüklenmesi, onaylı ve dijital olarak imzalanmış betik dosyalarının (* .ps1, * .py, makrolar vb.) çalıştırılması gerekmektedir.

5.7. Test

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

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	YAZILIM GELİŞTİRME ve TEMİN PROSEDÜRÜ	Doküman No	BGYS-PR26
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	09.07.2024
		Revizyon No	03
		Sayfa No	6 / 10

- Elde edilen uygulama yazılımının hem belirlenen gereksinimleri sağlayıp sağlamadığı hem de gerçekleştirimin beklentilere uygun olup olmadığını kontrol etmek için statik ve dinamik sınam tekniklerinden yararlanılır.
- Hazırlanan yazılımın ilk test aşaması proje ekibi tarafından lokal ortamda gerçekleştirilir.
- Tespit edilen eksiklikler giderildikten sonra sunucuya aktarım işlemi yapılır. Uygulama, iş 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.
- Geliştirme ve/veya test ortamında kullanılacak veriler gerçek veri olmamalıdır. Bu kapsamda, ilgili ortamlarda kullanılması için amaca uygun veriler üretilmelidir.

5.8. Hata ve Eksikliklerin Düzeltilmesi

Test sonunda bulunan hatalar ve eksiklikler yazılım ekibi tarafından düzeltilir. Yazılım hatasız bir şekilde çalışır duruma gelene kadar test ve hata ve eksiklerin düzeltilmesi süreci ardışık olarak devam eder.

5.9. İletişim ve Yayın

- Test aşamaları tamamlanan yazılım son kullanıcı seviyesinde kullanıma açılır.
- Uygulama; Yönetim ve son kullanıcılardan gelen taleplere göre belirli periyotlarla geliştirilmeye devam edilir.
- İşletim platformunda değişiklik yapılması gerektiğinde tüm süreç yazılım geliştirme ekibi tarafından yürütülür.
- Test süreci tamamlanıp hata ve eksikliklerden arındırılan yazılım yayına alınarak yazılım geliştirme süreci tamamlanır.

5.10. Güvenlik

Yazılım geliştirmenin tüm aşamalarında aşağıda belirtilen güvenlik maddeleri uygulanmalıdır:

- Uygulamaların kayıt altına aldığı veya kullandığı her türlü bilginin yetkisiz erişime kapalı olması gerekmektedir.
- Web, uygulama ve veri tabanı sunucularının sistem bileşenleri hakkındaki kritik bilgileri (sunucu adı ve sürümü, kullanılan program sürümü vb.) gizlenmelidir.
- Veri tabanı, uygulama sunucusu ve web sunucusu gibi kullanılan yazılımların güvenlik yamaları en üst seviyede olmalıdır.
- Kullanılan parolalar ve parolamı unuttum kontrol soru ve cevapları gibi diğer hassas veriler açık metin olarak saklanmamalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	YAZILIM GELİŞTİRME ve TEMİN PROSEDÜRÜ	Doküman No	BGYS-PR26
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	09.07.2024
		Revizyon No	03
		Sayfa No	7 / 10

- Uygulamalar, geliştirme ortamından test ortamına aktarılırken gereksiz olan dosyalar (örneğin test kodlar, demo programlar, yedek dosyalar) silinmeli, gerek yoksa kaynak kod aktarılmamalı ve aktarılabacak olan kaynak kodlardaki yorum satırları silinmelidir. Aktarım esnasında dosyalarda istenmeyen bir değişikliğin olmaması garanti edilmelidir.
- Uygulamada oluşan hatalar ve uygulama sunucusu ön tanımlı hata mesajları kullanıcıya detaylı olarak gösterilmemelidir.
- Uygulamaların üzerinde bulunduđu sunucular, servis verdikleri dizinlerin içeriklerini listelememelidir.
- 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.
- GET ve POST isteklerindeki HTTP parametreleri değiştirilerek üçüncü şahısların bilgilerine yetkisiz olarak erişilmemelidir.
- Uygulamayı çalıştıran sistem kullanıcısının, hizmet verilen dizin dışındaki yetkileri kaldırılmalıdır.
- Veri tabanı kullanıcısının sadece uygulamanın kullandığı veri tabanı kaynaklarına erişim hakkı olmalıdır.
- Sunucu üzerinde bulunan ve web tabanlı istatistik sağlayan uygulamalara erişim herkese açık olmamalıdır.
- Kısıtlı erişim gerektiren bütün URL'lere, servislere, uygulama verilerine, kullanıcı bilgilerine, güvenlik yapılandırma dosyalarına erişim denetlenmelidir.
- Yetki hakkının artık gerekmediği durumlarda (örneğin kurumdan ayrılma, projede rol değiştirme gibi) resmi yollarla en kısa sürede ilgili haklar iptal edilmelidir.
- Yönetim paneli gibi kritik dizinlerin isimleri kolay tahmin edilebilir olmamalıdır (admin, yönetici, administrator).
- Erişime açılan her kaynak kimlik denetimine tabi tutulma yöntemini de kullanmak zorundadır.
- Umumi olmayan bütün kaynaklara ve sayfalara erişim için sunucu tarafında kimlik doğrulaması yapılmalıdır.
- 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." şeklinde olabilir.
- Bütün başarılı ve başarısız login işlemleri ve kaynaklara erişim denemeleri kayıt altına alınmalıdır.
- Oturum bilgisi zaman aşımına uğrayacak şekilde yapılandırılmalıdır.
- Kurum dışına servislerle veri aktarımı yapılması durumlarında standart güvenlik prensiplerine uygun çalışılmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



Doküman No	BGYS-PR26
Yayın Tarihi	06.07.2015
Revizyon Tarihi	09.07.2024
Revizyon No	03
Sayfa No	8 / 10

- Güvenli yazılım geliştirme süreçleri ve uygunluk modellerinden faydalanılarak kurumsal yazılım geliştirme süreçleri güncellenmeli ve güvenli yazılım geliştirme yaşam döngüsü uygulanmalıdır.
- Devreye alınan veya güncellenen uygulamalarda sızma testleri ve uygulama güvenliği testleri yapılmalıdır. Tedarik edilen uygulamalar üzerinde sızma testleri gerçekleştirilmelidir. Kurumun kaynak koduna sahip olduğu tüm uygulamalar devreye alım öncesinde kaynak kod analizinden geçirilmelidir.
- Halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilgi; hileli faaliyetlerden, sözleşme ihtilafından ve yetkisiz ifşadan ve değiştirmeden korunmalıdır.
- Uygulamalar kullanıcı hesaplarının yönetimini sağlayan arayüzlere sahip olmalı ve bu arayüzlere yalnızca yetkili kullanıcıların erişebilmesi sağlanmalıdır. Kullanıcı hesapları, geçici (belirli bir süre, koşul vb. boyunca) veya kalıcı (aksi belirtilmedikçe sürekli) olarak kilitlenebilmelidir. Kalıcı olarak kilitlenen hesap üzerindeki geçici kilit kaldırılrsa dahi kilitli kalmalıdır.
- Kullanıcı tanımlamaları, yapılan işlemlerin izlenebilirliğini sağlayacak ve tekil olarak kişi veya sistemi işaret edecek şekilde yapılmalıdır.
- Kaynak kodda veya kaynak kod depolarında gizli bilgiler, API anahtarları ve parolalar yer almamalıdır. Kullanılan tüm kimlik doğrulama bilgileri şifrelenmeli ve korunan bir yerde depolanmalıdır. Açık anahtar altyapısı tabanlı kimlik doğrulama kullanılıyorsa özel anahtara sadece yetkili kullanıcının erişimine izin verecek mekanizmalar mevcut olmalıdır.
- Web uygulamalarının oturum çerezlerinde HTTPOnly, Secure, SameSite vb. bayraklar kullanılmalıdır. Tanımlama bilgilerinde depolanan oturum kimliklerinin yolları, uygulama için uygun kısıtlayıcı bir değere ayarlanmalıdır. Kullanıcılar uygulamadaki etkin oturumlarını görüntüleyebilmeli ve aktif oturumlarından istediğini sonlandırabilmelidir.
- Uygulamanın sahip olduğu sistem ve yapılandırma dosyaları ile denetim kayıtları ve iz kayıtları gibi bilgiler kullanıcı verisiyle aynı konumda (dizin, sistem bölümü vb.) depolanmamalıdır.
- Uygulama çok katmanlı mimari (multitier architecture) kullanılarak tasarlanmalı ve her katman için güvenlik mekanizmaları oluşturulmalıdır. Uygulamanın kullandığı veri tabanları ve kayıtlar, internetten doğrudan erişilemeyecek şekilde yapılandırılmalıdır. İnternete açık olarak çalışan sunucular (uygulama sunucusu, web sunucu, e-posta sunucuları vb.) DMZ (DeMilitarized Zone) gibi ayrı bir bölgede tutulmalıdır.
- Uygulama, tanımlanan güvenlik olaylarının/işlemlerinin (yetki değişiklikleri, kullanıcı değişiklikleri, kimlik doğrulama işlemleri) başarılı ve başarısızlık durumları için iz kayıtları oluşturabilmelidir. İz kaydı minimum şu bilgileri içermelidir: • İşlemi yapan kullanıcı (gerçek kişi veya yazılımsal süreç için tanımlanmış kullanıcı) bilgisi • İşlem zamanı • Kaynak ve hedef sistem tanımlayıcı bilgileri (ip, sunucu adı vb.) • İşlem özeti (başarılı işlem, başarısız işlem vb.).

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	YAZILIM GELİŞTİRME ve TEMİN PROSEDÜRÜ	Doküman No	BGYS-PR26
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	09.07.2024
		Revizyon No	03
		Sayfa No	9 / 10

- Kayıtların doğruluğunu sağlamak ve bütünlüğünün bozulmasını (log forging) engellemek için iz kayıtları oluşturulurken kullanılan girdiler üzerinde girdi denetimi yapılmalıdır. Kayıtlar görüntülenirken oluşabilecek zafiyetlere (XSS vb.) karşı ise karakter kodlama ve filtreleme gibi tedbirler uygulanmalıdır.
- Güvenilen bir sertifika otoritesinden her Transport Layer Security (TLS) sunucu sertifikasına bir güven zinciri oluşturulabilmeli ve internet üzerinden erişilebilen her sunucu sertifikası geçerli olmalıdır. Uygulama, Çevrimiçi Sertifika Durum Protokolü Damgalama (OCSP stapling) gibi yöntemlerle sertifika iptal denetimi gerçekleştirebilecek şekilde yapılandırılmalıdır. Web sayfalarına gerçekleştirilecek bağlantıların ve kullanılacak kaynakların güvenliği için HSTS kullanılmalıdır.
- Yapısal olmayan veriler (belirli bir formata/biçime sahip olmayan) için izin verilen karakterler ve uzunluklar belirlenerek verinin içeriğinde olabilecek olası zararlı karakterlere karşı girdi kontrolü yapılmalıdır.
- HTML form alanlarının veri girdileri, REST çağrıları, HTTP üst başlıkları, çerezler, toplu işlem dosyaları gibi veri girdileri için doğrulama denetimi yapılmalıdır.
- Uygulamanın girdi olarak kullandığı kişisel veri üzerinde girdi/çıktı doğrulama eksikliğinden kaynaklı zafiyetlere karşı güvenlik kontrolleri uygulanmalıdır.
- İlgili kişinin açık rızası olmadan kişisel veri web sayfalarının gizli alanlarında saklanmamalıdır. Kişisel veri, tarayıcı ön belleğinde (cache) saklanmamalıdır. Uygulamada kullanılan çerezlerin kişisel veri içermesi zorunluluk ise secure bayrağı (secure flag) kullanılmalıdır. Ayrıca, istemci tarafında web depolama (web storage) özelliği ile kişisel veriler kayıt altına alınmamalıdır.
- Kişisel veri üzerinde işlem yapılması ana amaç olmayan durumlarda (Adres bilgileri güncellenirken T.C. kimlik numarasının maskelenmesi, hesap numarasına havale işleminde alıcının adının maskelenmesi vb.) uygulama kişisel veriyi maskeleyerek göstermelidir.
- Kişisel verinin yetkisiz bir şekilde değiştirilmesini engellemek için uygun kriptografik yöntemler uygulanmalıdır.
- Özel nitelikli kişisel verinin işlenmesi ve kişisel verinin üçüncü kişilere aktarılması durumunda açık rıza uygulama üzerinden alınmalı ve açık rıza beyan durumu sorgulanabilmelidir.
- Uygulama üzerinde açık rıza metni yetkili kişiler tarafından güncellenebilmelidir. Güncelleme öncesindeki açık rıza metinleri saklanmalıdır. Güncellenen açık rıza metinleri için kullanıcılardan tekrar açık rıza alınması sağlanmalıdır.
- Bilginin korunması için Kriptografik Kontrollerin Kullanımı Politikası'na uygun hareket edilir. kriptografik anahtarların kullanımı sağlanmalıdır.
- Kurum tarafından onaylanmayan ve yazılım envanterine kaydedilmemiş yazılımlar kullanılmamalıdır. Envanterde olmayan yazılımlar, Bilgi Güvenliği ve Kalite Şube Müdürlüğü'ne danışılarak karşılıklı mutabık kalınırsa envantere eklenip kullanılabilir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	YAZILIM GELİŞTİRME ve TEMİN PROSEDÜRÜ	Doküman No	BGYS-PR26
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	09.07.2024
		Revizyon No	03
		Sayfa No	10 / 10

6. YAZILIM TEMİNİ

Yazılım temininde uyulması gereken güvenlik uygulamaları

- Yazılımı yapan yüklenici, kendisine devredilen işlerle ilgili her türlü bilgiyi (yazılım kaynak kodları, iş süreçleri, veri tabanı ile ilişkisel modeli gibi teknik dokümanları) gizli bilgi olarak kabul etmelidir ve idarenin yazılı izni olmadan üçüncü kişilere vermemeyi, açıklamamayı, kamuya duyurmamayı, değiştirmemeyi, birbirlerinin yetkilendirdiği kişilerin hizmetin ifası sırasında gerekli erişimlerini engellememeyi ve bu şekilde meydana gelecek sair davranışlardan kaçınmayı taahhüt etmelidir.
- Yazılımı yapan yüklenici kişisel verilerin mahremiyetini korumakla yükümlü olmalıdır.
- Uygulamanın ilgili yönetim arayüzlerine yalnızca yetkili kullanıcılar tarafından erişim sağlanmalıdır. Açık anahtar altyapısı tabanlı kimlik doğrulama kullanılıyorsa sertifika yolu doğrulanmalı ve kullanıcının sertifikası sistem üzerindeki geçerli kullanıcı veya grup bilgisi ile eşleştirilmelidir.
- Uygulamanın bileşenlerinin çalıştığı sunuculardan (web sunucusu, uygulama sunucusu vb.), kendi sınırları dışında bulunan / kendi kontrolünde bulunmayan veya ilişkili olmayan kaynak ve sistemlere uzak bağlantı ve erişim varsayılan olarak engellenmelidir. Aynı şekilde uygulama bileşenlerinin bulunduğu sunuculara uzaktan erişim izni kontrollü sağlanmalıdır.
- Açık kaynak kod tabanın zafiyete neden olacak şekilde değiştirilmesini engellemek için kod tabanı kurum bünyesinde barındırılmalıdır.
- Tedarik edilen veya hizmet alımı ile geliştirilen uygulamalar için yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde tedbir alınması sağlanmalıdır.
- Geliştirilen uygulama/sistem kapsamında sunulan arayüzün kullanıcılar tarafından açıkça anlaşılabilir olması adına Türkçe dil desteği sağlanmalı, tedarik edilen ürünlerde ise Türkçe dil desteği olan ürünler tercih edilmelidir.
- Sunulan web servisleri, girdi-çıkı denetimlerinin eksikliğinden kaynaklı saldırı çeşitlerine (XSS, uzak kod çalıştırma vb.) karşı önlem alacak şekilde geliştirilmeli ve konumlandırılmalıdır. Web servisi geliştirme aşamasında bilinen zafiyet içeren bileşenler (çatı, kütüphane, yazılım modülleri vb.) kullanılmamalıdır.
- Yeni geliştirmeler ve ürün/hizmet tedariki kapsamında kurumun fonksiyonel ve fonksiyonel olmayan testlere (yük, performans, güvenlik vb.) yönelik uygulanacak süreçleri tanımlı olmalı ve uygulanmalıdır. Bu süreçler düzenli olarak gözden geçirilmelidir. Alt yüklenici tarafından gerçekleştirilecek değişiklik ve sürüm yönetimi faaliyetleri kurumun politika ve prosedürleri ile uyumlu olmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi