BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

GELİŞTİRME VE DESTEK SÜREÇLERİ PROSEDÜRÜ

İçindekiler

1 Amaç

Bu doküman, bilgi güvenliğinin, bilgi sistemleri geliştirme yaşam döngüsü içerisinde tasarlanıyor ve uygulanıyor olmasını sağlamaktır.

2 Kapsam

Bu dokümanın kapsamı, Bilgi Güvenliği Kapsamı dokümanında yer alan tüm uygulama varlıklarını içerir.

3 Sorumluluk

Görev / Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
BGYS Birim Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi

5 İşlem Detayı

5.1 Güvenli Geliştirme Kuralları

Kurum iş süreçlerinin yürütmek için yazılımlar kullanmakta ve geliştirilmektedir. Sürekli gelişen ve değişen bu yazılımların süreçleri genel olarak kurum bünyesinde işletimi ve yükseltilmesi sağlanmaktadır. Nadiren dış kaynaklar üzerinden de geliştirilmektedir. Kurum bu süreçlerde BGYS prosedürleri, politikaları ve talimatları ile bilgi güvenliği gereksinimlerini sağlamayı ve geliştirmeyi amaçlamaktadır.

Güvenli geliştirme şartlarında kurum aşağıdaki kontrolleri uyulacaktır.

- Geliştirme yaşam döngüsü içerisindeki sistem değişikliklerinin kontrolü
- İşletim platformu değişikliklerinin kontrolü
- Yazılım paketlerindeki değişikliklerin kontrolü
- Güvenli sistem mühendisliği prensipleri
- Güvenli geliştirme ortamının sağlanması
- Dışarıdan sağlanan geliştirmelerin kontrolü
- Sistem güvenlik testleri
- Sistem kabul testleri
- Test verisinin korunması

5.2 Sistem Değişiklik Kontrolü

Değişim kontrollerinin uygulanması sistem bütünlüğünün sağlanması için zorunludur. Bu süreç, bir risk değerlendirmesi, değişikliklerin etkilerinin analizi ve gerekli güvenlik kontrollerini içerecektir. Değişiklik çalışmalarında sisteme gerektiği kadar erişim yetkisi, "Erişim Kontrol Politikası" na göre verilir. Değişim yönetiminde "İşletim Prosedürleri ve Sorumlulukları Prosedürü" ile ilişkili ve dikkat edilecek hususlar şunlardır;

- Yetki onay kayıtlarının saklanması
- Yetkinin yetkili kullanıcılar tarafından sağlanması
- Değişiklik gerektiren tüm yazılım donanım veri tabanının belirlenmesi
- Değişiklik ve değişikliğin içeriği için onay alınması
- Sistem ve işletim dokümanlarının güncellenmesi ve eski dokümanların arşivlenmesi
- Yazılım güncelleştirmelerinin sürüm değişikliklerinin ve kontrollerinin yapılması
- Değişikliklerin iş süreçlerini etkilemeyecek zamanlarda yapılması
- Değişiklikler için test ortamının kullanılması

5.3 İşletim Platformu Değişiklikleri Kontrolü

İşletim platformları değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir olumsuz etki olmamasını sağlamak amacıyla değişiklik öncesi kritik uygulamalar gözden geçirilecek ve test edilmelidir.

- İşletim platformundaki değişikliklerindeki tehlikeyi önlemek için platforma ait uygulama kontrolleri ve bütünlük prosedürleri incelenmelidir.
- İşletim platformlarındaki değişikliklerden önce testler için yeterli zaman ayrılmalıdır.

Değişikliklerden önce "**Bilgi Güvenliği İşletim Prosedürü**" 'ndeki Değişiklik Yönetimi gereklilikleri gözden geçirilir.

5.4 Yazılım Paketlerindeki değişiklikler

Yazılım paketlerindeki değişiklikler mümkün olduğunca kısıtlanır. İlgili sistem/uygulama yöneticileri yazılım paketlerindeki değişiklik ihtiyaçlarını gerekli durumlarda analiz eder. Değişiklik yapılması gerekli görülen alanlarda dikkat edilmesi gereken hususlar şunlardır;

- Satın alınan yazılımlarda üreticinin mevcut sürümden geçişte sorun olmayacağı onayının alınması
- Yeni gelişecek güncellemeler için uygunluğu
- Diğer yazılımlar ile arasındaki uyum
- Eski paketin saklanması
- Değişiklik kayıtlarının tutulması
- Yeni paketlerinin test ortamında işlevsellik kontrollerinin yapılması
- "Teknik Açıklıkların Kontrolü Prosedürü" ne göre testlerinin yapılması

5.5 Güvenli Sistem Mühendisliği Esasları

• Parola uygulamaları için "**Parola Politikası**" yayınlanmış ve içerisindeki esaslar uygulanmaktadır.

• E-posta esasları için "**İnternet ve E-posta Kullanım Prosedürü**" yayınlanmış ve içerisindeki esaslar uygulanmaktadır.

• Sistem yönetimi ve haberleşmesi uygulamaları için "**Teçhizat Güvenlik Prosedürü**", "**Bilgi Güvenliği İşletim Prosedürü**", "**Zararlı Yazılımlardan Korunma Prosedürü**", "**Yedekleme Prosedürü**", "**Olay Kaydetme ve İzleme Prosedürü**", "**Ağ Güvenliği Yönetimi Prosedürü**" yayınlanmış ve içerisindeki esaslar uygulanmaktadır.

• İş sürekliliği uygulamaları için "**Bilgi Güvenliği Sürekliliği Prosedürü**" yayınlanmış ve içerisindeki esaslar uygulanmaktadır.

• Erişim yönetimi uygulamaları için "**Erişim Kontrol Politikası**" yayınlanmış ve içerisindeki esaslar uygulanmaktadır.

• Ağ yönetimi uygulamaları için "**İnternet ve E-posta Kullanım Prosedürü**", "**Ağ Güvenliği Yönetimi Prosedürü**" yayınlanmış ve içerisindeki esaslar uygulanmaktadır.

• Bilişim olanakları kullanım ve yetkilendirmesi uygulamaları için "**Varlıkların Kabul Edilebilir Kullanım Politikası**" yayınlanmış ve içerisindeki esaslar uygulanmaktadır.

5.6 Doğrulama

1. Kamuya açık tüm sayfalar ve kaynaklarda kimlik doğrulaması zorunlu olması sağlanır.
2. Tüm şifreli giriş alanları için parolaları göstermemesi ve otomatik tamamlamanın devre dışı olması sağlanır.
3. Kimlik bilgileri ve diğer bilgilerin aktığı bağlantıların şifreli olarak yayınlanması sağlanır.
4. Parola yenileme işlemlerinde mevcut şifre veya yeni şifrenin şifreli olarak gönderilmesi sağlanır.
5. Uygulama tarafından kullanılan herhangi bir bileşende varsayılan kullanıcı adı parola (admin / password) kullanılmayacaktır.
6. Kullanıcı giriş ya da kayıt alanlarında bilgi veren hata mesajları gösterilmeyecektir.
7. Kimlik doğrulama için kaba kuvvet saldırılana karşı önlem alınacaktır.
8. Tüm kimlik kontrol tanımlamaları sunucu tarafında da yapılacaktır.
9. Kullanıcı parolalarında kurum standartların nitelikli parolalar oluşturulması zorunlu olacaktır.

5.7 Oturum Yönetimi

1. Kullanılan framework'ün oturum yönetimine sadık kalınacaktır.
2. Kullanıcı oturumunu kapattığında oturumların geçersiz olması sağlanacaktır.
3. Kullanılmayan oturumlar için zaman aşımı süresi belirlenecektir.
4. Kimlik denetimi yapılan tüm alanlarda güvenli çıkış olması sağlanacaktır.
5. Oturum ID'lerin çerezler dışında ifşa edilememesi (hata mesajları vb.) sağlanacaktır.
6. Oturum kapatıldığında çerezlerdeki ID bilgileri temizlenmeli ya da değiştirilmelidir.

7. Oturum sabitlenmesi engellemek için her oturum açıldığında oturum ID değiştirilmelidir.

5.8 Erişim Kontrolü

1. Kullanıcıların sadece yetkilendirildikleri alanlara eriştikleri kontrol edilecektir. (URL, Servis)
2. Hassas bilgi ifşa edecek hata bilgilerinin görüntülenmemesi sağlanacaktır.
3. Sunum katmanındaki yetkilendirmenin sunucu tarafında da aynı şekilde yetkilendirilmesi sağlanacaktır.
4. Tüm başarılı ve başarısız erişim kayıtları tutulacaktır.
5. Kullanıcının erişim kayıtları tutulacaktır.

5.9 Girdi Denetimi

1. Çalıştırma ortamı tampon taşmalarına (buffer overflows) izin vermemelidir ya da güvenlik kontrolleri bunu engellemelidir.
2. Çalıştırma ortamı SQL Injection, Cross Site Scripting, LDAP Injection, OS Command Injection izin vermemelidir ya da güvenlik kontrolleri bunu engellemelidir.
3. Girdi karakter setinin tüm kaynaklar için UTF-8 olduğu doğrulanacaktır.
4. Tüm girdi denetimi hataları kayıt altına alınacaktır.

5.10 Hata Yönetimi ve Loglama

1. Uygulama logları güvenilir bir kaynaktan zaman damgası ile kayıt altına alınmalı ve log kayıtları en az istek IP adresi, kullanıcı bilgisi, olay zamanı bilgilerini içermelidir.
2. Log kayıtları izinsiz değiştirilmelere karşı korunmalıdır.
3. Log kayıtlarının tek standartta alınması sağlanmalıdır.

5.11 Veri Koruma

1. Hassas bilgileri içeren tüm formların otomatik tamamlama özellikleri ve istemci tarafında önbelleğe alınması iptal edilecektir.
2. Hassas verinin URL üzerinden gönderilmemesi, http mesaj body bölümünde gönderilmesi sağlanmalıdır.

3. Uygulama kullanıcıların normalden daha sık yaptıkları isteklere tepki vermelidir. (Örneğin: belirli sürede belirli sayıda aynı işlem yapılmasına izin verilmesi)

5.12İletişim Güvenliği

1. Aktarım kaynağında kullanılan sertifikaların otoriteler (CA) tarafında onaylanıyor olması
2. Hassas veri aktarımı ve girişlerde TLS kullanılması.

5.13HTTP güvenliği

1. Uygulama üzerinden erişim yöntemlerini belirlenecek (Post, Get) kullanılmayan yöntemlerin erişimi engellenecektir.
2. Http yanıtlarının başlıkları güvenli karakter kümesi içinden seçilecektir.

5.14Kötü Niyetli Kod Kontrol

Uygulamaya dışarıdan entegre edilen kod, kütüphane, ayar dosyalarının güvenilir kaynaktan alındığı kontrol edilecektir.

5.15Dosya ve Kaynaklar

1. Başka bir siteye yönlendirme esnasında uygulamanın hassas bilgilerinin taşınmasının engellenmesi sağlanacaktır.
2. Güvenilir olmayan kaynaklardan gelen dosya ya da klasör adları temizlenerek “prevent local file inclusion attack” engellenmesi sağlanacaktır.
3. Dış kaynaklardan elde edilen dosyalar anti virüs yazılımları ile kontrol edilerek sisteme dâhil edilecektir.
4. Güvenilir olmayan kaynaklardan gelen kodlar çalıştırılmayacaktır.

5.16Güvenli Geliştirme Ortamı

Güvenli geliştirme ortamına ilişkin, insan, süreç ve teknoloji odak alınarak riskler belirlenir ve önlemler alınır. Bu bağlamda yeni sistem geliştirmeleri yapılırken aşağıdaki konu başlıkları dikkate alınır;

- Sistem tarafından işlenen, iletilen saklanan verilerin hassaslığı
- Yasal ve düzenleyici gereksinimler, iç ve dış taraf gereksinimleri

- Hali hazırda uygulanan güvenlik önlemlerinin durumu
- İlgili sistem geliştirme alanlarında/projelerinde güvenilir insan kaynağının çalıştırılması
- Sistem geliştiriminde ne ölçüde dış kaynak kullanılacağı
- Diğer geliştirme ortamlarından ayırım ihtiyacının belirlenmesi
- Geliştirme ortamına erişim kontrolü
- Geliştirme ortamındaki değişiklerin izlenmesi
- Yedeklerin güvenli alanlarda saklanması

5.17Dışarıdan Sağlanan Geliştirme

Sistem/yazılım geliştirmede dış kaynak kullanımında tedarikçi zinciri göz önünde bulundurularak aşağıdaki konular dikkate alınır;

- Lisans anlaşmaları, kodlara kimin sahip olacağı, fikri mülkiyet haklarına ilişkin çerçeve şartnamede belirlenecektir.
- Güvenli tasarım, güvenli kodlama ve test yöntemleri şartnamede belirlenecektir.
- Sistem kalite ve güvenlik kabul gereksinimleri şartnamede belirlenecektir.
- Gerekli testlerin yapıldığına dair kayıt sunma yöntemleri şartnamede belirlenecektir.
- Kaynak kod anlaşmaları şartnamede belirlenecektir.
- Geliştirme süreçlerinin denetleme hakkı şartnamede belirlenecektir.
- Geliştirici onaylı tehdit modeli isteği şartnamede belirlenecektir.
- Geliştirme esnasında yapılan güvenlik testleri, zararlı kod analizleri ve bu testlere ait sonuçların kayıt olarak istenmesi şartnamede belirlenecektir.
- Uygulamanın işletilmesi yönetilmesi ve bakımı için gerekli işletim dokümanlarının gerekliliği şartnamede belirlenecektir.
- Tabi olunan kanunlar için uygunluğuna ait onay belgesi şartnamede belirlenecektir.

Yukarıda belirtilen kontrollerden gerekli olanlar bilgi güvenliği toplantılarında belirlenerek şartnamelere eklenir.

5.18Sistem Güvenlik Testi

Yeni geliştirilen veya güncellenen sistemler/uygulamalar üzerinde testler gerçekleştirilecektir. Bu testler sistemlerin beklenen şekilde çalıştığının doğrulanması için gerçekleştirilir.

Geliştirme kurum bünyesinde gerçekleştiriliyorsa, bu testler geliştirme ekibi tarafından yapılır. Sistemlerin kritikliğine göre kurum içinde veya dış kaynak kullanılarak geliştirilen sistemler bağımsız bir kuruluş tarafından her türlü güvenlik ve uygunluk testine tabi tutulur. Bu süreç de "Bilgi Sistemlerinin Güvenlik Gereksinimleri Prosedürü" ve sistem kabul testleri maddesi de referans alınır.

5.19 Sistem Kabul Testi

Sistemler kabul komisyonuna girmeden önce tüm testler yapılır. Sitem testleri için otomatik test araçları kullanılabilir.

- Sistem zafiyetlerini kontrol etmek için zafiyet analiz yazılımları ile test edilir.
- İşlevsellik testleri uygulamayı kullanacak birim tarafından kontrol edilir.
- Kod üzerindeki zafiyetler bilgi güvenliği toplantılarında kararlaştırılması durumunda yapılır.
- Test gerçeğe en yakın ortamda test edilir.
- Test sonuçlarının incelenmesinde tüm paydaşlar ile görüş birliğine varılır.
- Test sonuçları bilgi güvenliği toplantılarında değerlendirilir. Değerlendirme sonuçlarına göre yeniden geliştirme ve test süreçleri başlatılabilir.

5.20 Test Verisi

Canlı sistemde kullanılan, kullanıcı kimlik bilgileri ya da kişisel bilgilerin test amaçlı kullanımından mümkün olduğunca kaçınılır. Kişisel bilgilerin test amaçlı kullanımı gerekli ise, değişime ve silinmeye karşı korunur.

Operasyonel verilerin test sırasında kullanımında aşağıdaki konu başlıkları göz önünde bulundurulur;

- Hassas veri maskeleme yazılımı ile maskelenir ya da gerçek veri kullanılmaz.
- Canlı sistemde uygulanan erişim kontrol esasları, test ortamında da uygulanır.
- Canlı sistem verilerinin, test ortamına aktarılmasında ayrı bir yetkilendirme uygulanır.
- Testlerin tamamlanmasını takiben, canlı ortam verileri, test ortamından silinir.
- Canlı ortam verilerinin kopyalama işlemleri, loglanır ve kayıt altına alınır.

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					