BGYS POLİTİKASI

Politika Numarası	PLTK-09
Politika Tanımı	Güvenli Geliştirme Politikası
Amaç ve İlkeler	Bilgi güvenliğinin, yazılım ve sistemlerin güvenli geliştirme yaşam döngüsü içinde tasarımlanmasını ve uygulanmasını sağlamaktır.
Sorumluluklar	**Bilgi İşlem Personeli:** İlgili tarafların bu politikada belirtilen gereksinimlere uygun hareket edip etmediğinin kontrolü ve yönlendirilmesinden sorumludur. **Tedarikçiler**: Bu politikanın şartlarına uygun hareket etmekten sorumludur.
Sapma ve Özel Durumlar	Bu politikanın ihlali, sözleşme şartlarına uygun olmayan durumlara bağlı olarak yasal takibata neden olabilir.

UYGULAMA

1. Geliştirme, test ve üretim ortamlarının ayrılması

Yazılım geliştirme, test ve üretim ortamlarının ayrılması ve yönetimi, dış kaynaklı yazılım geliştirme firmalarının sorumluluğundadır. Sistemsel geliştirmeler ve entegrasyonlar Bilgi İşlem personelleri koordinasyonunda gerçekleştirilecektir.

Dış kaynaklı yazılım geliştirme firmalarıyla yapılan sözleşmelerde, geliştirme, test ve üretim ortamlarının ayrılması ve güvenliği ile ilgili detaylı şartlar ve gereksinimler belirtilmelidir.

Sistemsel geliştirmeler ve entegrasyonlar için şirket içinde ayrı bir ekip bulundurulmalıdır. Bu ekip, geliştirme, test ve üretim ortamlarının ayrılmasını sağlamak için uygun yöntemler ve protokolleri belirlemeli ve uygulamalıdır.

Şirket içindeki sistemsel geliştirme ve entegrasyon süreçlerinde, geliştirme, test ve üretim ortamları arasında ayrım sağlanarak geliştirme sürecinde yapılan değişikliklerin test ve üretim ortamlarına etkisi minimize edilmelidir.

Şirket içi sistemsel geliştirme ekipleri, geliştirme, test ve üretim ortamlarının ayrı ayrı yönetilmesi ve güvenliğinin sağlanması için gereken teknik altyapı oluşturulmalı ve sürekli olarak güncellemelidir.

2. Yazılım geliştirme yaşam döngüsündeki güvenlik konusunda rehberlik

Yazılım geliştirme süreçleri dış kaynaklı yazılım firmaları sorumluluğunda gerçekleştirilmekte olup bu süreçte rehberlik sağlamak ve etkin önlemlerin alınması için gerekli destek sağlanmalıdır.

3. Şartname ve tasarım aşamasındaki güvenlik gereklilikleri

Yazılım geliştirme süreçlerine destek olmak amacıyla şartname ve tasarım aşamasında güvenlik gerekliliklerinin uygulanması sağlanacaktır. Bu kapsamda güvenlik gerekliliklerinin belirlenmesi, risk değerlendirmesi, güvenlik tasarımı, güvenlik testleri ve değerlendirmeleri kapsayacak şartlar ortaya konmalıdır.

4. Projelerdeki güvenlik kontrol noktaları

Projelerin başlangıcında güvenlik gereksinimleri belirlenmeli ve belgelendirilmelidir.

Proje yöneticileri ve ekip üyeleri, güvenlik konularında düzenli olarak eğitim alınıp ve güvenlik bilinci geliştirilmelidir.

Proje sırasında, yazılım ve sistemler düzenli olarak güvenlik testlerinden geçirilip güvenlik açıkları tespit edilmeli ve düzeltilmelidir.

Projeler tamamlandıktan sonra, dış denetçiler tarafından güvenlik denetimleri gerçekleştirilip ve projenin güvenlik standartlarına uygunluğu değerlendirilmelidir.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
19.04.2018	01/25.01.2024	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

5. Regresyon testi, kod tarama ve sızma testleri gibi sistem ve güvenlik testleri

Güvenlik odaklı bir yaklaşım benimsenerek süreçlerin güvenilirliğini ve güvenliğini sağlamak için ilgili tedarikçilerle iş birliği yapılmalıdır. Bu doğrultuda ilgili tedarikçilerin regresyon testi, kod tarama ve sızma testi gibi işlemleri gerçekleştirdiği doğrulanmalıdır.

6. Kaynak kodu ve yapılandırma için güvenli depolar

Tedarikçilerin kaynak kodu ve yapılandırma için güvenli depoları sağlama faaliyetleri gerçekleştirme durumu doğrulanmalıdır. Bu doğrultuda yazılım geliştirme hizmeti alınan firmalardan kaynak kodu ve yapılandırma dosyalarının güvenliğini sağlamalarını talep edilmelidir. Tedarikçiler, bu dosyaların yetkisiz erişime karşı korunduğunu, bütünlüğünü korumak için güvenli depolarda saklandığını ve sadece yetkili personelin erişimine açık olduğunu ispatlamalıdır.

7. Sürüm kontrolünde güvenlik

Dış kaynaklı yazılım geliştirme hizmeti alınan firmaların, sürüm kontrolü yönetimini etkin bir şekilde gerçekleştirmesi ve güvenliği sağlaması beklenmektedir. Tedarikçilerin, sürüm kontrolü sistemlerinin güvenlik önlemlerini içeren bir politika veya prosedürler setine sahip olduğunu, yetkisiz erişimleri önlediğini, değişiklikleri izlediğini ve izlediği sırada veri bütünlüğünü koruduğunu belgelemesi gerekmektedir.

8. Gerekli uygulama güvenliği bilgisi ve eğitimi

Yazılım geliştirme hizmeti alınan dış firmalardan, çalışanlarının güvenlik bilinci ve uygulama güvenliği konularında eğitim aldıklarını ve güncel bilgiye sahip olduklarını belgelemesi gerekmektedir.

9. Geliştiricilerin güvenlik açıklarını önleme, bulma ve düzeltme yeteneği

Hizmet alınan tedarikçilerin güvenlik açıklarını önleme, bulma ve düzeltme konularında yetkinlik düzeylerini gösteren hususları belgelemesi gerekmektedir.