REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH
01	2022 versiyon değişikliği	01.10.2024

1. AMAÇ

Bu prosedür; Aksaray Üniversitesi bilgi güvenliğinin, bilgi sistemlerinin tüm yaşam döngüsü boyunca dâhili bir parçası olmasını, geliştirme yaşam döngüsü içerisinde tasarlanıyor ve uygulanıyor olmasını ve test için kullanılan verinin korunmasını sağlamak maksadıyla uygulanan yöntemleri anlatmak, alınacak tedbirleri açıklamak üzere düzenlenmiştir.

2. KAPSAM

Bu prosedür; Bilgi Güvenliği Yönetim Sistemi kapsamında alınacak tüm sistem temini, geliştirme ve bakım tedbirlerini ve bu tedbirlerin uygulanmasına ait yönetimini kapsar.

3. UYGULAMA

3.1 SİSTEM TEMİNİ, GELİŞTİRME VE BAKIMI

3.1.1 Bilgi Sistemlerinin Güvenlik Gereksinimleri

3.1.1.1 Bilgi Güvenliği Gereksinimleri Analizi ve Belirtimi

- ✓ Temin edilecek bilgi sistem teçhizatı ilgili riskler göz önüne alınarak güvenlik gereksinimleriyle birlikte değerlendirilir.
- ✓ BT donanım ve yazılım güvenlik ürünleri (Firewall, Switch, Kriptografik özellikli ürünler vb.) tedarik edilirken mümkün oldukça Common Criteria EAL sertifikalı çözümler tercih edilir.
- ✓ BT donanım ve yazılım güvenlik ürünleri temin edilirken en az 2 yıl garanti ve destek koşulu ile garanti süresi içinde ve sonrasında yedek parça temini edebilme koşulları göz önüne alınmaktadır.
- ✓ Sunucu / PC / WS / NB alımlarında Common Criteria EAL sertifikasına sahip bilgisayar üreticilerinin ürünleri tercih edilmektedir.
- ✓ Kurumumuz BT donanım ve yazılım güvenlik ürünleri test ve kabul işlemleri aşağıdaki yöntemlerle yapılmaktadır.
  - Ürünlerin işlevselliği açısından belirlenen güvenlik gereksinimlerinin karşılanıp karşılanmadığına ait test raporları ilgili tedarikçi firmadan istenir.
  - Ürünlerin testleri ilgili tedarikçi firma ile birlikte POC çalışması yapılır.
  - Ürünlerin kabulü; ürünlerin işlevselliği açısından belirlenen güvenlik gereksinimlerinin Kabul seviyesinde POC çalışmasının sonunda karşılanması ile yapılır.

3.1.1.2 Halka Açık Uygulama Servislerinin Güvenliği

- ✓ Halka açık ağlar üzerinden sistemlere erişimler ilgili ağlar üzerinden geçen hassas verilerin gizlilik ve bütünlüğünün korunması için IPSec VPN kullanılarak yapılmaktadır.
- ✓ Herkese açık bilgiler kanunlar çerçevesinde toplanır ve yayınlanır.
- ✓ Herkese açık hassas bilgi toplanırken, işlenirken ve saklanırken gerekli koruma önlemleri alınır.

3.1.1.3 Uygulama Hizmet İşlemlerinin Korunması

- ✓ E-Defter ve E Fatura hizmet uygulamalarında iletişim kriptografik yöntemler ile korunmaktadır.
- ✓ Tüm tarafları kapsayan sorumluluklar gizlilik sözleşmeler ile koruma altına alınmıştır.
- ✓ Tüm taraflar arasındaki haberleşme yolunun şifrelenmesi, doğrulanması için gerekli kontroller uygulanmaktadır.

3.2 Geliştirme ve Destek Süreçlerinde Güvenlik

3.2.1 Güvenli Geliştirme Politikası

- ✓ Yazılım geliştirme aşamalarında ele alınacak güvenlik gereksinimleri BS/BP/022 Güvenli Yazılım Geliştirme ve Test Prosedüründe belirlenmiş ve uygulanmaktadır.
- ✓ Yeni ve güncellenmiş sistemler geliştirme süreci boyunca teste ve doğrulamaya tabi tutulur.

3.2.2 Sistem Değişiklik Kontrolü Prosedürleri

- ✓ Uygulama değişiklik kontrolleri ile ilgili tasarım aşamalarından tüm bakım çalışmalarına kadar uygulamalar ve ürünlerin bütünlüğünü sağlamak için aşağıda belirlenen değişiklik kontrolleri uygulanmaktadır,
  - Uzlaşıya varılmış yetki seviyelerinin bir kaydının tutulması,
  - Değişikliklerin yetkili kullanıcılar tarafından yapıldığının temin edilmesi,
  - Değişikliklerden zarar görmemelerini temin etmek için kontrollerin ve bütünlük prosedürlerinin gözden geçirilmesi,
  - Uygulama teknik dokümanı her bir değişiklikte revize edilir.
  - Tüm yazılım güncellemeleri için bir versiyon kontrolü yürütülmektedir.
  - Tüm değişiklik istekleri BGYS/BF/026 Modifikasyon İhtiyaç Formu ile yönetilmektedir.

3.2.3 İşletim Platformu Değişikliklerden Sonra Uygulamaların Teknik Gözden Geçirilmesi

- ✓ İşletim platformları değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş kritik uygulamalar aşağıdaki hususlara göre gözden geçirilmektedir;

- ✓ İşletim platformu değişikliklerine ilişkin uygulama öncesinde, uygun test ve gözden geçirmelere imkân tanımak için öncesinde değişiklikler ilgili tüm kullanıcılara bildirim yapılır.
- ✓ Değişikliklerin iş sürekliliği planlarına etkisi incelenir ve gerekiyorsa İş sürekliği planlarına ilişkin uygun değişiklikler yapılır.

3.2.4 Yazılım Paketlerindeki Değişikliklerdeki Kısıtlamalar

- ✓ Mümkün ve uygulanabilir oldukça, tedarikçi tarafından sağlanan yazılım paketleri değiştirilmeden kullanılmaktadır.

- ✓ Bir yazılım paketinin değiştirilmesi gerekli görüldüğünde, aşağıdaki noktalar göz önünde bulundurulmaktadır;
  - Yerleşik kontrollerin ve bütünlük proseslerinin (Örneğin yazılım paketinde yapılan değişiklik bir güvenlik zafiyeti yaratıyor olabilir) ele geçirilme riski,
  - Üreticinin onayının alınmasının gerekip gerekmediği,
  - Üreticiden gerekli değişikliklerin standart program güncellemeleri olarak temin edilebilme olasılığı,
  - Değişikliklerin sonucu olarak, yazılımın gelecekteki bakımı konusunda yükümlülük altında kalması halinde oluşacak etki.
  - Kullanılmakta olan diğer yazılımlar ile uyumluluk.

3.2.5 Güvenli Sistem Mühendisliği Esasları

- ✓ Kurumumuz Güvenli Sistem Mühendisliği Prensipleri 3 ana başlık altında Risk tabanlı ve Katmanlı güvenlik yaklaşımı ile birleştirilmiştir.

  - Güvenlik Temelleri
  - Güvenlik ile ilgili hususlar tüm sistem tasarımının en önemli parçası olarak belirlenmiştir.
  - Yazılım geliştiriciler güvenli yazılım geliştirilmesi konusunda yeterli yetkinliğe sahip olmalıdır.

1. <u>Risk Tabanlı Yaklaşım</u>

- ✓ Proje devreye alınması sırasında ortaya çıkabilecek riskler kabul edilebilir seviyelere düşürülmelidir.
- ✓ Dış sistemler ilk aşamada güvensiz şekilde değerlendirilir.
- ✓ Bilgi işlenirken, taşınırken ve saklanırken korunmalıdır.
- ✓ Her türlü saldırı için önlemler göz önüne alınmalıdır.

2. <u>Katmanlı Güvenlik Yaklaşımı</u>

- ✓ Erişim Katmanı = Kullanıcı kimlik doğrulama seviyeleri, kullanıcı erişim kısıtlamaları, kullanıcı rol tanımları belirlenmesi, şifre politikaları, halka açık sistemler üzerinden kritik sistemlere erişimin sınırlandırılması, en düşük ayrıcalık uygulaması vb.
- ✓ Teknoloji Katmanı = Sadece güvenilir olan sektörde fonksiyonları ve güvenilirliği kanıtlanmış cihazlar/yazılımlar kullanılması
- ✓ Direnç katmanı = Açıklıkların azaltılması, Yüksek erişilebilirlik ve felaket kurtarma çözümleri
- ✓ Kayıt katmanı = Loglama, kayıt saklama

Kurumumuz, Güvenli Sistem Mühendisliği Prensipleri aşağıda belirtilen proje aşamaları için uygulanmaktadır.

- ➢ Başlangıç

- Planlama
- Uygulama Devreye Alma
- İzleme
- Kapanış

✓ Dış veya İç kaynaklı olarak devreye alınan tüm bilgi teknolojileri projelerinde ve bilginin işlenmesi, transferi ve depolanması konularında Doğal felaketler, teknolojik veya insan kaynaklı tehditler göz önünde bulundurulmaya çalışılmaktadır.

✓ Projelerin devreye alınması aşamasında "BGYS/BF/005 Proje Risk Yönetim Değerlendirme Test ve Kabul Formu" ile değerlendirme yapılmaktadır.

3.2.6 Güvenli Geliştirme Ortamı

✓ Kurumumuz da Güvenli bir geliştirme ortamı; sistem geliştirme ve uyumu ile ilişkili insanları, prosesleri ve teknolojiyi kapsamaktadır.

✓ Aşağıdaki hususları dikkate alarak bağımsız sistem geliştirme çalışmaları ile ilişkili riskler değerlendirmekte ve özel sistem geliştirme çalışmaları için güvenli geliştirme ortamları oluşturmaktadır;

- Sistem tarafından işlenen, depolanan ve iletilen verinin hassaslığı,
- Uygulanabilir dış ve iç gereksinimler, örneğin; düzenlemeler veya politikalardan,
- Ortamda çalışan personelin güvenilirliği
- Sistem geliştirme ile ilişkili dış kaynak kullanım derecesi,
- Farklı geliştirme ortamları arasındaki ayrım ihtiyacı,
- Geliştirme ortamına erişim kontrolü,
- Ortamdaki ve ortamda depolanmış koddaki değişikliklerin izlenmesi,
- Yedeklerin güvenli yerlerde saklanması,
- Verinin ortama ve ortam dışına olan hareketlerinin kontrolü.

3.2.7 Dışarıdan Sağlanan Geliştirme

✓ Sistem geliştirme dış kaynaklı olduğunda, aşağıdaki hususlar kuruluşun tüm dış tedarik zinciri için dikkate alınmaktadır;

- Dış kaynaklı tedarik içeriği ile ilişkili lisans anlaşmaları, kod mülkiyeti ve fikri mülkiyet hakları
- Güvenli tasarım, kodlama ve test uygulamaları için sözleşme gereksinimleri
- Çıktıların kalitesi ve doğruluğu için kabul testleri,
- Dağıtım üzerinde hem kasıtlı hem de kasıtsız zararlı içerikten korunmak için uygulanan yeterli test etme kanıtının temini,
- Bilinen güvenlik açıklarının varlığına karşı korunmak için yeterli derecede test yapıldığına dair kanıtların temini,
- Kaynak kodu temini hususları yapılan sözleşme içerisinde belirlenmektedir.

- Geliştirme prosesleri ve kontrolleri ile ilgili sözleşmeden doğan denetim hakkı,
- Dışarıdan sağlanan geliştirme hizmetine ait dokümantasyon,
- Kuruluş, uygulanabilir yasalar ve verimlilik doğrulama kontrolünün uyumundan sorumludur.

3.2.8 Sistem Güvenlik Testi

- ✓ Yeni ve güncelleştirilmiş sistemler, bir dizi koşul altında test girdileri ve beklenen çıktıların ve faaliyetlerin detaylı bir programının hazırlanmasını kapsayan geliştirme prosesleri süresince doğrulama ve test yapılmaktadır.
- ✓ Kurum içi geliştirmeler için bu tür testler başlangıçta geliştirme ekibi tarafından yapılmaktadır.
- ✓ Bağımsız kabul testleri (hem dış kaynaklı hem de kuruluş içinde) yalnızca sistemin sadece beklendiği gibi çalışmasını sağladıktan sonra yapılmaktadır.

3.2.9 Sistem Kabul Testi

- ✓ Sistem kabul testi, bilgi güvenliği gereksinimlerini ve güvenli sistem geliştirme aşamaları ile uyumluluğu içermektedir.
- ✓ Testler temin edilen bileşenler ve bütünleşik sistemler üzerinde yapılmaktadır.
- ✓ Gerekli görüldüğü takdirde kod analiz araçları veya açıklık tarayıcıları gibi otomatikleştirilmiş araçlarda kullanılabilmektedir.

3.3 Test Verisi

3.3.1 Test Verisinin Korunması

- ✓ İşletimsel uygulama sistemlerine uygulanan erişim kontrolleri test uygulama sistemleri içinde uygulanmaktadır.
- ✓ Test maksadı ile test sistemine operasyon bilgisinin her kopyalanışında yetkilendirme gözden geçirilir, kullanımı kaydedilir.
- ✓ Test işlemi tamamlanmasının hemen ardından işletimsel bilgiler test sisteminin güncellenme zamanına kadar muhafaza edilebilmektedir.

4. SORUMLULUK

Kapsam dâhilindeki tüm personel Sistem Temini, Geliştirme ve Bakım Prosedürü uygulama esaslarına uygun hareket etmekle yükümlüdür.

5. EK

BGYS/BF/026 Modifikasyon İhtiyaç Formu

BGYS/BF/005 Proje Risk Yönetim Değerlendirme Test ve Kabul Formu

BS/BP/013 Güvenli Yazılım Geliştirme ve Test Prosedürü