REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH
01	2022 versiyon değişikliği	01.10.2024

1. AMAÇ

Bu prosedür; Aksaray Üniversitesi bilgi işleme tesislerinin doğru ve güvenli işletimlerini, bilgi ve bilgi işleme tesislerinin kötücül yazılımlardan korunmasını temin etmek, veri kaybına karşı koruma sağlamak, olayları kaydetmek ve kanıt üretmek, İşletimdeki sistemlerin bütünlüğünü temin etmek, teknik açıklıklardan yararlanılmasını engellemek, tetkik faaliyetlerinin işletimdeki sistemler üzerindeki etkilerini asgariye indirilmesini sağlamak ve bu maksatla uygulanan yöntemleri anlatmak, alınacak tedbirleri tanımlamak üzere düzenlenmiştir.

2. KAPSAM

Bu prosedür; Bilgi Güvenliği Yönetim Sistemi kapsamında alınacak tüm İşletim Güvenliği tedbirlerini ve bu tedbirlerin uygulanmasına ait yönetimini kapsar.

3. UYGULAMA

3.1 İŞLETİM GÜVENLİĞİ

3.1.1 İşletim Prosedürleri ve Sorumlulukları

3.1.1.1 Yazılı İşletim Prosedürleri

- ✓ Yedekleme ve geri yükleme kuralları Yedekleme talimatında tanımlanmıştır.
- ✓ Kapsam içindeki BT Altyapısı içerisindeki teçhizat üzerinde konfigürasyon ve kurulum işlemleri sadece Bilgi Teknolojileri personeli tarafından yapılmaktadır.
- ✓ Yazıcılara gönderilen Hassas bilgi içeren yanlış işlerin çıktılarının imhası için kâğıt kırpma cihazları kullanılmaktadır. Çalışanlarda bu konuda farkındalık yaratılmıştır.
- ✓ Beklenmeyen operasyonel veya teknik güçlükler karşısında iletişime geçilecek kurum ve Yetkililerinin listesi BGYS/BF/001 İlgili Taraf Beklentiler ve İletişim Formu tanımlanmıştır.
- ✓ Sistem kayıt bilgileri ve denetim takibi yapılmaktadır.
- ✓ Sistemde arıza meydana geldiğinde; sistemi yeniden başlatma ve kurtarma ile ilgili gerekli işlemlere ait yöntemler iş sürekliliği planlarında tanımlanmıştır.

3.1.1.2 Değişiklik Yönetimi

- ✓ Bilgi güvenliğini etkileyen, iş prosesleri, bilgi işleme tesisleri ve sistemlerdeki yapılacak değişiklikler; öncesinde tanımlanır, planlanır, test edilir ve devreye alınır.
- ✓ Yapılacak değişiklikler hakkında ilgili tüm personele değişiklik detayları bildirilmektedir.
- ✓ Değişikliklerle ilgili tüm personelin görüşü alınarak, güvenlik etkileri de dahil olmak üzere potansiyel etkileri değerlendirilir.
- ✓ Değişiklik teklifleri "BGYS/BF/026 Modifikasyon İhtiyaç Formu" kullanılarak yapılmaktadır.

3.1.1.3 Kapasite Yönetimi

- ✓ Bilgi ve İletişim Teknolojileri ekipman ve alt yapı kapasite ve kaynak planlamaları ile ilgili sistemler izlenmekte olup, Kontroller esnasında tespit edilen yüksek kaynak kullanımlarına göre ihtiyaçlar belirlenmekte ve kapasite gereksinimleri ile ilgili kestirimler yapılarak kaynak ve kapasite planlamasına yönelik rapor yönetim onayına sunulmaktadır.
- ✓ İhtiyaç yönetim tarafından onaylandıktan sonra uygun olarak tedarik edilir.
- ✓ Anahtar konumundaki sistem kaynaklarının kullanım durumu sistem yöneticileri tarafından sürekli izlenir.
- ✓ Uygun durumlarda Bilgi ve İletişim Teknolojileri ekipman ve alt yapı kapasite ve kaynak planlamaları ile ilgili aşağıdaki yöntemlerde uygulanmaktadır:
    - Kullanılmayan verinin silinmesi (disk alanı)
    - Uygulamaların, sistemlerin, veri tabanlarının ya da ortamların hizmetten çıkarılması,
    - Toplu proseslerin ve zamanlamaların optimizesi,
    - Uygulama mantığının ya da veri tabanı sorgularının optimize edilmesi,
    - Eğer iş kritik değilse kaynak tüketen hizmetler için reddetme ya da bant genişliği sınırlaması (örneğin; video akışları)
- ✓ Kapasite ve kaynak planlaması yapılırken gerekli durumlarda insan kaynakları kapasitesi, ofis ve tesisler de göz önünde bulundurulur.

3.1.1.4 Geliştirme, Test ve İşletim Ortamlarının Birbirinden Ayrılması

- ✓ Geliştirme, test ve işletim ortamları, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmıştır.
- ✓ İşletimsel sorunları önlemek için gerekli olan işletim, test ve geliştirme ortamları arasındaki ayrım aşağıdaki hususlar göz önüne alınarak yapılmaktadır;
    - Geliştirme ortamında yapılan yazılım ile canlı ortamda çalışan yazılımının çalıştığı işletim sisteminin bulunduğu ortamlar ayrılmıştır.

- Geliştirme ortamındaki yazılımın canlı ortama aktarılması ile ilgili kurallar tanımlanmıştır.
- Geliştirme ortamında yapılan yazılım değişiklikleri canlı ortam da çalışan yazılım üzerine uygulanmadan önce test edilmektedir. İstisnai durumlar dışında, testler işletimdeki sistemler üzerinde yapılmamaktadır.

3.2.1 Teçhizat Kötücül Yazılımlardan Koruma

3.2.1.1 Kötücül Yazılımlara Karşı Kontroller

- ✓ Yerel yönetici hakları kullanıcı yetkilerinden alınmıştır. İstisnai durumlar hariç kullanıcılara yerel yönetici hakkı verilmemektedir.
- ✓ Kullanılan tüm yazılımlar yönetim tarafından onaylanmış lisanslı yazılımlardır.
- ✓ Sadece bilgi işlem bölümü personeli gerekli yazılımları bilgisayarlara yükleyebilirler.
- ✓ Bilinen ya da şüphelenilen kötücül web sitelerini tespit etmek ve önlemek için gerekli kontroller uygulanmaktadır.
- ✓ Kara listeler takip edilerek kötü niyetli yazılım ve-veya SPAM mail yayan adreslerden mail alınması engellenir.
- ✓ Tüm bilgisayarlarda güncel virüs tarama ve temizleme yazılımı otomatik çalışacak şekilde yüklenip ayarlanmıştır.
- ✓ İnternetten indirilen dosyalar, e-postalar ve ekleri e-posta sunucusunda kötü niyetli yazılımlara karşı tarandıktan ve temizlendikten sonra network de kullanıma sunulur.
- ✓ Bilgisayar kullanıcıları kötü niyetli yazılımla karşılaştıklarında ne yapacakları konusunda bilgi sahibidir.
- ✓ Kötü niyetli yazılımların meydana getirdiği hasarların iş sürekliliğinin aksatmaması için geri kurtarma ve yedekleme tedbirleri alınır.

3.3.1 Yedekleme

3.3.1.1 Bilgi Yedekleme

- ✓ Yedek alma, yedekten geri dönme ve geri yükleme testi ile ilgili hususlar BS/BP/014 Yedekleme Planı Prosedüründe tanımlanmıştır. Yedek alma yöntemleri, Yedeklerin türünü (örneğin; tam veya diferansiyel yedekleme) ve sıklığını içermektedir. (Kullanıcı bilgisayarlarında bulunan Gizli ve Kritik bilgilerin sunucu üzerine alınması ile ilgili tanımlama yapılacak. Aynı zamanda yedekleme sorumluluğunun da kullanıcılarda olduğu talimatta yapılacak tanımlamalar da tanımlanacak)
- ✓ Yedekleme yöntemleri ve yedek saklama süreleri mevcut teknik altyapı ve ihtiyaçlar doğrultusunda belirlenmektedir.
- ✓ Yedeklemeler, merkezde bir felaketten dolayı görülecek hasardan kaçınmak için yeterli bir mesafede ve/veya özel veri saklama kasasında muhafaza edilmektedir.
- ✓ Kullanıcı bilgisayarlarındaki bilgilerin asıllarının dosya sunucusunda muhafaza edilmesi kullanıcı

sorumluluğundadır.

- ✓ Alınan yedeklerin ve yedekleme ortamının ihtiyaç olduğunda doğru bir şekilde çalışmasını sağlamak için düzensiz aralıklarla farklı ortamlara yedekten geri dönme testleri yapılmaktadır.
- ✓ Yedekten geri dönme ve geri yükleme testlerine ait işlemler Yedekten geri dönme listesi ile kayıt altına alınmaktadır.
- ✓ Yedekleme ve yedekten geri dönüş işlemleri sadece yetkili bilgi teknolojileri personeli tarafından yapılır.
- ✓ Gizliliğin önemli olduğu durumlarda, yedekleme şifreleme yoluyla yapılabilir.
- ✓ Kritik sistemler ve hizmetlerin bir felaket durumunda yeniden çalışır duruma getirilmesi ile ilgili planlamalar İş Sürekliliği planlarında ele alınmıştır.

3.4.1 Kaydetme ve İzleme

3.4.1.1 Olay Kaydetme

- ✓ Kullanıcı kimliği, log-on ve log-off olduğu tarih ve zaman kayıtları,
- ✓ Hangi IP hangi bilgisayar tarafından kullanılmış,
- ✓ Başarılı ve reddedilmiş sistem, uygulama erişim girişimlerinin kayıtları,
- ✓ Başarılı ve reddedilmiş, veri ve diğer kaynaklara erişim girişimlerinin kayıtları,
- ✓ Sistem yapılandırma değişikliklerine ait kayıtlar

3.4.1.2 Kayıt Bilgisinin Korunması

- ✓ Kayıt bilgisi saklanmaktadır. İzleme dosyalarının saklanma ortamlarının dolması durumunda başarısız kaydetme veya eski kayıtların üzerine yazma olmaması için gerekli önlemler alınmaktadır.
- ✓ Kaydedilen mesajların değiştirilmemesi sağlanır.

3.4.1.3 Yönetici ve Operatör Kayıtları

- ✓ Sistem yöneticisi ve operatörlerin faaliyetleri kayıt altına alınır.
- ✓ Olay ve hata günlükleri yetkisel bazda korunarak saklanmaktadır.
- ✓ Sistem yöneticisinin hangi kullanıcı hesapları üzerinde çalıştıkları kayıt altına alınır.
- ✓ Sistem yöneticilerine ait kayıtlar Bilgi Teknolojileri Yöneticisi tarafından gözden geçirilir.
- ✓ Operatörlere ait kayıtlar sistem yöneticileri tarafından gözden geçirilir.

3.4.1.4 Saat Senkronizasyonu

- ✓ Tüm sistemler belirli bir zaman sunucusu ile senkronize olmaktadır. (Sunucular, Kamera sistemleri, Giriş-Çıkış sistemleri vb.)

3.5 İşletimsel Yazılımın Kontrolü

3.5.1 İşletimdeki Sistemler Üzerine Yazılım Kurulumu

- ✓ Yazılım uygulamaları ve program kütüphanelerinin güncellemesi yetkin uzman personel tarafından uygun yönetim yetkisi altında yapılmaktadır.
- ✓ İşletimdeki sistemlerde sadece çalıştırılabilir onaylı kod bulunmaktadır, geliştirme kodu ya da derleyiciler bulunmamaktadır.
- ✓ İşletimsel program kütüphanelerinin tüm güncellemelerinin bir denetim kaydı tutulmaktadır.
- ✓ Değişiklikleri uygulamadan önce bir geri alma stratejisi olarak değişiklik öncesi mevcut durumu yedeklenmektedir.
- ✓ Uygulama yazılımının önceki sürümleri bir acil durum önlemi olarak saklanmaktadır,
- ✓ Uygulama ve işletimsel sistem yazılımları sadece kapsamlı ve başarılı bir şekilde test edildikten sonra uygulanmaktadır; testler, kullanılabilirliği, güvenliği, diğer sistemlere etkiyi ve kullanıcı dostluğunu kapsayıp, ayrı sistemler üzerinde yapılmaktadır.
- ✓ Yazılımının eski sürümlerine ait tüm gerekli bilgi, parametreler, prosedürler, yapılandırma detayları yasal mevzuatlar dikkate alınarak yazılım kullanıldığı sürece arşivde saklanmaktadır.
- ✓ Bilgi güvenliği açıklıklarının azaltmasına ya da kaldırılmasına yardımcı olmak için yazılım yamaları uygulanmaktadır.

3.6 Teknik Açıklıkların Yönetilmesi

3.6.1 Teknik Açıklıkların Yönetimi

- ✓ İşletim sistemlerinin güvenlik güncellemelerine ait takip yapılmaktadır.
- ✓ Sunucuların işletim sistemi güvenlik güncellemeleri riskler göz önüne alınarak manuel yönetilmektedir.
- ✓ Meşru kaynaklarda yayınlanan bir yama varsa, yama yükleme ile ilgili riskler değerlendirilir.
- ✓ Yamaların, etkinliğinden emin olmak ve geri dönülemez etkilerle sonuçlanmasından kaçınmak için sisteme yüklenmesi gereken yamalar test edilerek değerlendirildikten sonra sonuca göre sisteme yüklenir.
- ✓ Kritik güncellemeler düşük riskli sistemlerde uygulanır. Sorun çıkmaması durumunda yüksek riskli sistemlerde de uygulanır.
- ✓ Sistem denetim kayıtları (log) tutulur.

3.6.2 Yazılım Kurulumu Kısaltmaları

- ✓ Kullanıcıların Local Admin hakları alınarak yazılım kurulumları kısıtlanmıştır.
- ✓ En az ayrıcalık prensibi uygulanmaktadır.
- ✓ Mevcut yazılımların güvenlik yamaları ve güncellemelerinin kullanıcılar tarafında otomatik yüklenmesi için izin verilmiştir.

3.7 Bilgi Sistemleri Tetkik Hususları

3.7.1 Bilgi Sistemleri Teknik Kontrolleri

- ✓ Sızma testleri (teknik zafiyet testleri) kurumumuz tarafından yaptırılmakta ve kayıtları saklanmaktadır.
- ✓ Teknik açıklık testleri mesai saatleri dışında yapılmaktadır.
- ✓ Teknik açıklık testi ile ilgili tüm erişimler izlenmekte ve kaydedilmektedir.
- ✓ Tetkik testler, yazılım ve veriye sadece okunabilir erişim olacak şekilde sınırlandırılmaktadır.

4. SORUMLULUK

Kapsam dâhilindeki tüm personel İşletim Güvenliği Prosedürü uygulama esaslarına uygun hareket etmekle yükümlüdür.

5. EK

BS/BP/014 Yedekleme Planı Prosedürü

BGYS/BF/026 Modifikasyon İhtiyaç Formu

BGYS/BF/001 İlgili Taraf Beklentiler ve İletişim Formu