MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

BİLGİ GÜVENLİĞİ İŞLETİM PROSEDÜRÜ

İçindekiler

1 Amaç

Bu dokümanın amacı İşletim Prosedürleri ve Sorumlulukları ile kurum bilgi işleme olanaklarının doğru ve güvenli işletiminin teminini sağlamak.

2 Kapsam

Bu doküman, Bilgi Güvenliği Kapsamı dokümanında yer alan tüm bilgi 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. Yazılı İşletim Prosedürleri

Birimlerde yürütülmekte olan iş süreçlerine ve işletilen sistemlere ait dokümantasyon tarafından "**Doküman Yönetim Prosedürü**" ne göre hazırlanır.

İşletim prosedürleri örnek olarak "**Yedekleme Prosedürü**", "**Olay Kaydetme ve İzleme Prosedürü**", "**İnternet ve E-posta Kullanım Prosedürü**" olmak üzere hazırlanmış ve yayınlanmıştır.

Güncelliği sağlamak amacıyla işletilen sistemlere ait detay işletim dokümantasyonu için üreticilerin web sitelerinde bulunan talimatlar kullanılır.

Kurum çalışanları tarafından hazırlanan dokümantasyonu, ihtiyacı olan tüm kullanıcılar için ilgili dosya sunucusu veya BGYS uygulaması üzerinden erişebilir durumdadır.

Bilişim olanaklarının kabul edilebilir kullanımına ait esaslar "**Varlıkların Kabul Edilebilir Kullanım Politikası**" tanımlanmıştır.

5.2. Değişiklik Yönetimi

Yürütülen iş faaliyetlerinin kesintiye uğramasını önlemek amacıyla işletim sistemlerinde görülen her değişiklik gerekli test işlemleri yapıldıktan ve onay verildikten sonra uygulamaya geçmelidir. Bu tür onay için kullanılan yöntemlerde yürürlükteki güvenlik kontrolleri de dâhil olmak üzere olası etkiler de dikkate alınmalıdır.

Değişiklik yöntemi, gerektiğinde değişikliğin yarıda kesilmesi ve başarısız değişikliklerden geri dönmek için hangi eylemlerin yapılması gerektiğinin tanımlanması için vazgeçme seçeneğine de sahip olmalıdır. Yapılan tüm değişikliklerin tam olarak belgeye geçirilmesi gerekir. Örneğin; konuyla ilgili tüm bilgiyi içeren bir denetim kaydı.

Sistemin işleyişini etkilemesi muhtemel olabilecek önemli değişiklikler, olası etkiler ve güvenlik kriterleri değerlendirilerek otomasyon yazılımları veya birim yöneticisinin onayı veya değişikliği gerekçesiyle açıklayan e-posta veya "**Değişiklik Kontrol Form**"u ile birim yöneticisine bilgi verilerek yapılır.

Değişiklikten etkilenen birimlere/personele duruma göre yazı / e-posta ile bilgi verilir.

Kritik veya hassas sistemlerdeki değişiklikler test sistemlerinde test edilir, testlerin başarılı sonuçlanması durumunda gerçek ortama alınır.

5.3. Kapasite Yönetimi

Kapasite yönetim süreci sürekli olmalı ve gereksinimlerin belirtimi güvenilir hesaplamaların yapılmasına imkân verecek standart bir biçimde ortaya konulmalı ve belgelenmelidir.

Kurumda kapasite planlaması için monitoring yazılımı kullanılmaktadır. Bu yazılımlar üzerinden sistem bileşenleri kontrol edilebilmektedir. Kontrol adımları olarak bileşen bazlı ram, disk, işlemci, bağlantı süreleri kontrol edilmektedir.

Hizmetler veya verilen servislerle ilgili, sunucuların, sistem ve ağ cihazlarının üstündeki ağ (network), sabit disk, hafıza ve işlemci kullanımları gibi kaynakları izlenir, ihtiyaç duyulması halinde kapasite artırımı için çalışma yapılır. Kapasite planlama işlemi yılda en az bir (1) kez "Kapasite Planları" ile gerçekleştirilir

5.4. Geliştirme, Test ve İşletim Ortamının ayrılması

İşletim ortamdaki yetkisiz erişim ve değiştirmeye ilişkin riskleri azaltmak adına aşağıdaki konu başlıkları göz önünde bulundurulur.

Geliştirme, test ve işletim ortamları, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için mümkün olduğu sürece birbirinden ayrılır.

Yazılım geliştirme projelerinde, geliştirme ortamları yazılım geliştiren kullanıcıların bilgisayarları olmasıyla ayrıştırılmıştır.

Yazılım geliştirme projelerinde kritik tüm uygulamalar için ayrı test ortamları oluşturulur; ayrı test ortamı olmayan kritik uygulamalar risk analizinde değerlendirilir.

Her sunucu/sistem için ayrı test ortamı olmamakla birlikte sanal ortamda oluşturulmuş test ortamlarında veya test için belirlenmiş kullanıcı bilgisayarları/sunucularında testler gerçekleştirilir.

Revizyon Kayıtları

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