1. AMAÇ

Bu politika, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı sistem alımı, geliştirme ve bakım ilkelerini oluşturmayı amaçlar.

2. KAPSAM

Bu politika, Karamanoğlu Mehmetbey Üniversitesinin Bilgi İşlem Daire Başkanlığı bilişim sistemi alımı, geliştirme ve bakımını kapsamaktadır.

3. SORUMLULAR

- Bilişim Sistemi Kullanıcıları
- Bilgi İşlem Daire Başkanlığı

4. TANIMLAR

5. UYGULAMA

5.1 Bilişim Sistemlerinin Güvenlik Gereksinimleri

Bir bilişim sistemindeki güvenlik gereksinimleri, sistem satın alma, geliştirme veya değişikliği sürecinin gereksinim belirleme ve analiz fazında tanımlanır ve dokümante edilir. Bu gereksinimler iş süreci sahipleriyle birlikte doğrulanır ve kararlaştırılır.

Sistem güvenlik gereksinimleri, sürece dâhil edilen bilgi varlıklarının (Varlık Yönetimi bölümüne uygun olarak) varlık değerini ve yeterli güvenlik önlemi olmamasından kaynaklanabilecek olası zararları yansıtır.

5.2 Uygulamaların Bilgiyi Doğru İşlemesi

- Uygulama geliştirme ve bakım süreci için güvenlik gereksinimlerini içeren resmi bir yöntem belirlenip dokümante edilir.
- Uygulamalara veri girişi gerçekleştirilirken verinin doğruluğu ve uygunluğu kontrol edilir. Bunun için uygun kontroller yapılır ya da kontrolü sağlamak için uygun yazılımlar satın alınır.
- Uygulamalarda, hatalar ya da kasıtlı eylemlerden ötürü bozulan bilginin tespiti için doğrulama kontrolleri oluşturulur.
- Uygulamalarda bilginin aslına uygunluğunun ve veri bütünlüğünün sağlanmasına yönelik gereksinimler ve bu gereksinimlere uygun kontroller belirlenir ve bu kontroller uygulanır.
- Uygulamadan veri çıkışı, bilginin koşullara uygun olarak işlenip işlenmediği ve saklanıp saklanmadığı kontrol edilir.

5.3 Sistem Dosyalarının Güvenliği

- Yazılımın işletim sistemleri üzerindeki kurulumunun kontrol edilmesi için ilgili prosedürler uygulanır.

- Test verisi dikkatli şekilde seçilir, korunur ve kontrol edilir.
- Şirket içerisinde mevcut program kaynak kodu, erişim kısıtlanarak saklanır ve yalnızca Bilgi İşlem Müdürü ya da Atanan İcra Kurulu üyesinin onay verdiği yetkili personelin erişimine izin verilir.

5.4 Geliştirme ve Destek Süreçlerinde Güvenlik

Değişiklik yönetimi için resmi prosedürler uygulanır. Önerilen tüm sistem değişikliklerinin hayata geçirilmesi için başlangıç ve bitişi süreçlerinde onaylanması zorunludur ve sistemin veya işletim ortamının güvenliğine zarar vermediğini kontrol etmek için gözden geçirilir. İşletme için kritik olan uygulamalar, işletim sistemi yamaları veya güncellemeleri kurulmadan önce kontrol edilir ve test ortamında test edilip onaylanır. Kritik uygulamalar için test ortamı ile canlı ortamın ayrı olması esastır. Herhangi bir üçüncü taraf yazılım paketinde yapılması gerekli tüm değişiklikler (konfigürasyon değişiklikleri, raporlardaki değişiklikler vb. değişiklikler de dâhil) Program Değişikliği Kontrolü Prosedürlerine göre gerçekleştirilir.

Yazılımın üçüncü kişi tarafından geliştirilmesi durumunda, aşağıdakiler yapılır:

- Üçüncü kişinin uyguladığı yazılım geliştirme süreçlerinin Şirketin Bilişim Sistemi Alım, Geliştirme ve Bakım Metodolojisi'ne uyumlu olmaları sağlanır.
- Uygulamanın kalite ve doğruluğu için uygun lisans anlaşmalarına ve sözleşme gereksinimlerine sahiptirler
- Üçüncü kişilerden, yapılan işin kalitesi ve doğruluğuna yönelik güvence alınır.
- Kaynak kodunun sahipliği (fikri mülkiyet hakları) alınır. Eğer bu üçüncü kişi için mümkün değilse, kod bir sözleşme ile sahiplenilir.
- Yapılan işin kalite ve doğruluğunu denetlemek için gerekli erişim hakları temin edilir.
- Test süreçleri gerçekleştirilir.

Şirket dışına giden verilerin incelenmesi sağlanır ve dışarıya bilgi sızmasını önlemek için periyodik olarak sistem faaliyetleri izlenir.

5.5 Teknik Zafiyet Yönetimi

Kullanılan bilişim sistemlerinin teknik zafiyetleri ile ilgili bilgi zamanında temin edilir, şirketin bu gibi zafiyetlerden ne kadar etkileneceği değerlendirilir ve bunlara bağlı riskleri adreslemek için uygun önlemler alınır.

6. İLGİLİ DOKÜMAN

- Bilişim Sistemi Alımı, Geliştirme ve Bakımı Prosedürü
- Kabul Edilebilir Kullanım Politikası