1. AMAÇ

Bu politika, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde yapılan iletişim ve operasyonların belirli ilkeler kapsamında yapılması amaçlanmıştır.

2. KAPSAM

Bu politika, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde yapılan iletişim ve operasyonlarını kapsar.

3. SORUMLULAR

- Bilgi İşlem Daire Başkanlığı ve Birimleri

4. TANIMLAR

Operasyon; İşlem
Administrator; Yönetici
NTP (Network Time Protocol); Ağ zamanlama protokolü

5. UYGULAMA

5.1 Operasyon Prosedürlerinin Dokümantasyonu

Kurum, sistem, ağ, güvenlik ve uygulama yöneticilerinin (administrator) günlük işlerini yapmalarını sağlamak amacıyla Kurumun tüm Bilgi İşlem süreçlerine yönelik işletme prosedürleri oluşturulur ve prosedürlerin güncelliği sağlanır.

5.2 Operasyonel Değişiklik Yönetimi

Bilgi İşlem varlıklarındaki (uygulamalar, sunucular, sistem yazılımı, güvenlik mimarisi ve ağ cihazları vb dâhil) değişiklikler, ilgili risklerin kabul edilebilir bir seviyede yönetildiğinden emin olmak için kontrollü şekilde yapılır. Değişikliğin doğru şekilde yönetilmesi için; değişiklik önceden planlanır ve plana uygun şekilde geliştirilir, değişiklik etki analizi yapılır, değişiklik canlıya alınmadan önce test edilir, değişikliğe başlanması ve tamamlanması için onay alınır ve tüm değişiklik süreci dokümanlarının güncel olması sağlanır. Değişiklikler canlı ortam haricinde bir ortamda test edilir ve hata görülürse değişiklik geri alınır.

İstisnai durumlarda gerçekleştirilmesi gereken acil değişiklikler ve izlenecek acil durum süreci için uygun prosedürler uygulanır.

5.3 Operasyonel Prosedürlerde Görevler Ayrılığı İlkesi

Bütün Bilgi İşlem Birimi süreçlerinde görevler ayrılığı ilkesine en üst seviyede uyulur. Herhangi bir olayın başlatanı ile onaylayanı ayrıdır. Aşağıdaki maddelere uyulur:

- Operasyonel işler ile görevli kişilere, sistem yönetimi ile ilgili sorumluluklar verilemez.

- Test süreçlerinde görevli olan kişilere, sistem yönetimi ile ilgili sorumluluklar verilemez.
- Sistemlerdeki güvenlik ve süreçlerin gözden geçirme sorumluluğu, sistemin geliştirilmesinden, bakımından ve sistem veya süreç kullanımından bağımsızdır.

Görevlerin ayrıştırılmasının mümkün olmadığı durumlarda telafi edici kontroller konulur. Örneğin; aktivitelerin izlenmesi, denetim izlerinin kontrol edilmesi, vb.

5.4 Geliştirme, Test ve Canlı Ortam Aktivitelerinin Ayrıştırılması

Canlı sistemdeki yetkisiz, onaysız değişiklik riskinin azaltılması için geliştirme, test ve canlı ortam aktiviteleri fiziksel ve mantıksal olarak ayrıştırılır.

Geliştirme, test ve canlı ortam arasındaki bilgi akışları kontrol edilir.

5.5 Ağ Güvenlik Yönetimi

Bkz. Ağ Güvenliği Politikası (Bilgi Güvenliği Prosedürleri "Ağ Güvenliği Yönetimi")

5.6 Bilgi Paylaşımı

Kurum kritik bilgi varlıklarının kaybolmasını, zarar görmesini veya hatalı kullanımını önlemek için, bilgi varlıkları ve yazılımlarının 3.kişiler ve organizasyon dışı kişiler ile paylaşılmasını kontrol eder.

Bilgi ve Yazılım Paylaşım Anlaşması

Kritik bilgi varlıklarının veya yazılımların Kurum dışı kişiler ile paylaşılması ile ilgili bir paylaşım anlaşması ya da gizlilik sözleşmesi imzalanır. Bu paylaşımı yapacak Kurum bölümü, bu anlaşmadaki sorumlulukları alır. Bu anlaşma , hem fiziksel hem de elektronik paylaşımları kapsar ve paylaşılacak kritik bilginin hassasiyetini ve ne seviyede korunması gerektiğini içerir.

Bu anlaşmalarda yönetim sorumlulukları, bildirim gereksinimleri, ambalaj ve iletim standartları, kurye kimlik bilgileri, sorumlulukları ve yükümlülükleri, veri ve yazılım sahipliğini, koruma sorumlulukları ve alınması gereken önlemleri, tüm şifreleme gereksinimleri belirtilir.(Örneğin Kurumun test edeceği ya da Kavram Kanıtlama(PoC) işlemleri için yapacağı her çalışmada, çalışmanın sahibi birim ile çalışmayı yapacak firma arasında gizlilik sözleşmesi imzalanır.

Fiziksel Ortam Transferi

Bilgi içeren fiziksel ortamlar, Kurumun fiziksel sınırları dışına çıkarılırken ya da bir lokasyondan başka bir lokasyona taşınırken zarar görmeye veya yetkisiz bir şekilde erişilmeye karşı korunur ve takip altına alınır. Transfer öncesi ilgili yöneticinin ve Bilgi Güvenliği Yöneticisinin onayı alınır ve bir üst onay için Bilgi İşlem Müdürüne gönderilir.

Elektronik Mesajlaşma ve E-Posta Güvenliği

Elektronik mesajlaşma ve e-posta güvenliği ile ilgili hususlar Kabul Edilebilir Kullanım Politikası'nda tanımlanmıştır.

Bilişim sistemlerinin 3. kişi sağlayıcılara açılmaları durumunda bilginin korunması için gerekli güvenlik önlemleri uygulanır.

5.7 İzleme, Denetleme ve Denetleme İzlerinin Tutulması

Kullanıcı faaliyetleri, istisnalar ve güvenlik olaylarının denetim izleri tutulur ve izlenir. Denetim izleri aşağıdakileri içerir:

- Başlangıç ve bitiş zamanları(sunucu, kullanıcı, DB seviyesi logları vb)
- Sistem hataları veya aksaklıkları ve alınan düzeltici önlemler
- Veri dosyalarının ve sistem çıktılarının doğrulanması ve doğru bir şekilde işlenmesi
- Denetim izi tutulan kişinin adı veya kullanıcı ismi
- Erişim düzeyi yüksek (sistem yöneticileri ve sistem operatörleri gibi ayrıcalıklı kullanıcılar) kullanıcıların aktiviteleri kayıt altına alınmalı ve bağımsız biri tarafından düzenli olarak gözden geçirilir.
- Kritik uygulamalara erişimler ile Kurum ağına erişimler herhangi bir güvenlik ihlaline karşı Bilgi Güvenliği Yöneticisi ve Sistem ve Ağ yönetmeni tarafından izlenir. Bu gibi durumlar için uygun mekanizmalar kurulur. Güvenlik ihlali durumunda acilen Bilgi İşlem Müdürüne bilgi verilir
- Denetim izleri, kayıt tutma ve saklama ihtiyaçlarına göre tutulur.
- Denetim izi tutma mekanizmaları ve denetim izleri yetkisiz erişimlere karşı korunur.

Kurum bünyesindeki bütün sistemlerin sistem saatleri, NTP (Network Time Protocol) sistemi ile eş hale getirilir. EKS, (Endüstriyel Kontrol Sistemlerinin, Kurum içi Bilişim sistemlerinden izole olması açısından NTP saati yerine ayrı bir uydu anteni ile kendi sistem saatini güncellemektedir.

5.8 Sistem Dokümanlarının Güvenliği

Sistem dokümanları, yetkisiz erişimlere karşı korunur.

Sistem ya da uygulama sahibi, sistem dokümanlarının paylaşımını ve dağıtımını Bilgi İşlem Şube Müdürü ile birlikte onaylar. Bu dokümanlar sadece ihtiyaç duyan personel ile paylaşılır.

5.9 Kötü Niyetli ve Mobil olan Kodlara Karşı Koruma Politikası (Anti-virüs Koruması)

Kurum ağı, tüm sunucuları, masaüstü bilgisayarları, iş istasyonları, el cihazları ve ağ geçitleri kötü niyetli erişimlere karşı korunur.

Anti-virüs uygulamaları ve süreçleri erken tanı, etkin koruma ve kötü niyetli kod erişimlerine karşı etkin bir koruma sağlar.

Kötü niyetli faaliyetlerle ilgili kullanıcı bilinçlendirme programları uygulanır.

Mobil kodların (solucan, truva atı vb.) çalıştırılmasını engelleyecek kontroller konulur.

6. İLGİLİ DOKÜMAN

- Bilgi Güvenliği Politikası
- İletişim ve Operasyon Yönetimi Prosedürü