1. AMAÇ

Bu politika, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı olay yönetimi ilke ve kurallarını oluşturmak amaçlar.

2. KAPSAM

Bu politika, Karamanoğlu Mehmetbey Üniversitesinin Bilgi İşlem Daire Başkanlığı olayların tamamını kapsamaktadır.

3. SORUMLULAR

- Bilgi İşlem Daire Başkanlığı
- Sistem Yönetimi Birimi

4. TANIMLAR

- USOM: Ulusal Siber Olaylara Müdahale Merkezi
- SOME: Siber Olaylara Müdahale Ekibi

5. UYGULAMA

5.1 Bilgi Güvenliği Olaylarının ve Zayıflıkların Raporlanması

Olay, kuruma ait olan bilginin ya da bilişim sisteminin gizlilik, bütünlük veya erişilebilirliğinin zarar gördüğü durumun oluşmasıdır. Bu potansiyele sahip ve maddi anlamda çok büyük bir hasara sebep olabilecek istisnai durumlarda yönetimin de sürece dâhil olması gereklidir.

Güvenlik açıkları (bilişim sistemlerinin gizlilik, bütünlük ve erişilebilirliğinin zarar görmesi), bilgi güvenliği ihlaline sebebiyet veren yazılım hataları ve kurumun güvenlik politikalarının ve prosedürlerinin ihlal edilmesi de bir olay olarak kabul edilir.

Karşılaşılan olaylar, bu olayların zamanında çözülmesi ve gelecekte karşılaşılmaması için gerekli mercilere ve USOM ‘a bildirilir ve önleyici aksiyonlar alınır.

Bütün personel ve üçüncü kişi sağlayıcılar da bilgi güvenliği olayları prosedürü hakkında farkındalığı oluşturulur (güvenlik ihlalleri, tehditler, zafiyetler ve arızaları).

Bildirilen bütün olaylar kayıt altına alınır, analiz edilir ve önceden bildirilmiş kriterlere göre sınıflandırılır.

Bilişim sistemleri ve servislerini kullanan bütün çalışanlar, geçici personeller ve üçüncü kişi sağlayıcılar güvenlik zayıflıkları ile karşılaştıklarında ya da şüphelendiklerinde bu durumu Bilgi Yöneticisine ya da birim yöneticisine doğrudan, e-posta, telefon, fax vb iletişim araçlarıyla bildirirler.

Olayların sınıflarına göre aksiyon alınır, USOM’a ve ilgili kuruluşlara bildirilir ve eskalasyon süreci de bu sınıflara göre yapılır. (Bilgi Güvenliği Prosedürleri “Bilgi Güvenliği Olay Yönetimi ”)

5.2 Yetkililer ile İletişime Geçilmesi

İhtiyaç duyulması durumunda yetkili makamlardan uygun kişiler ile irtibata geçilir. (Bilgi Güvenliği Prosedürleri "Siber Olaylara Müdahale Ekip Üyeleri ")

5.3 Bilgi Güvenliği Olaylarının Yönetimi ve İyileştirilmesi

Bilgi güvenliği olaylarına hızlı, etkin ve düzgün yanıt sağlanması için yönetimin sorumlulukları ve gerekli prosedürler uygulanır.

Bilgi güvenliği olaylarının sonucunda olayların tekrarını engelleyecek öğrenimleri sağlayan mekanizmalar oluşturulur. Olaylardan kaynaklanan etkinin derecesi ve maliyeti ölçülür ve izlenir. Bilgi İşlem birimine ve Bilgi Güvenliği Yöneticisine bilgi güvenliği kapsamında ilgili eğitimler verilir ya da bu eğitimleri almaları Kurumca sağlanır.

Bir kişinin ya da kurumun, bilgi güvenliği olaylarından kanuni bir işleme (sivil ya da cezai) tabi tutulması durumlarına karşı, olay ile ilgili kanıtlar kurallara uygun bir şekilde toplanıp saklanır.

Bilgi güvenliği dokümanlarının ihlali durumunda kurum çalışanları kurum Personel Yönetmeliği'nde yer alan disiplin hükümlerine tabidirler.

6. İLGİLİ DOKÜMAN

- Ağ Güvenliği Prosedürü
- Kabul Edilebilir Kullanım Politikası