KONYA
SANAYİ ODASI

KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI

KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI

1.0 Amaç

Bu politika Kurum çalışanlarının, bilgi güvenliliği ve iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dahilinde gerekli müdahale yapabilmelerine yönelik standartları belirlemektedir. İzlenen olayın uygun şekilde raporlanması ve belirlenen önlem ve acil durum faaliyetlerinin uygulanması önemlidir.

Kurum çalışanlarının, bilgi güvenliği veya iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dahilinde gerekli müdahaleyi yapabilmelerine yönelik normlar aşağıda belirtilmiştir.

2.0 Kapsam

Bahse konu acil durum senaryoları yaşanmadan önce uygun acil durum hareket planının yapılması esastır. Bilgi güvenliğine yönelik tehlike senaryolarından bazıları sistemlere yapılacak direkt saldırılar, zararlı kod içeren programların, kişilerin sisteme sızması, bilginin hırsızlığı, dışarıdan veya içeriden gerçekleştirilebilecek saldırı öncesi taramalar olarak tanımlanabilir.

3.0 Politika

a) Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir. Sorumlular odamız Koruma Planında Teknik Koruma Grubunda belirtilmiştir.
b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin, uygulama veya veri tabanı sunucularında donanım ve yazılıma ait problemler oluştuğunda, yerel veya uzak sistemden yeniden kesintisiz (veya makul kesinti süresi içerisinde çalışma sağlanabilmelidir.
c) Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlaması için aynı ortamda yerel kopyalama (lokal replication) veya pasif sistem çözümlerini hayata geçirilebilir.
d) Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmalıdır.
e) Acil durumlarda sistem log'ları incelenmek üzere saklanmalıdır.
f) Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.
g) Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
h) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
i) Acil Durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır:
    - Seviye A: Bilgi kaybı. Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi.
    - Seviye B: Servis kesintisi. Kurumsal servislerin kesintisi veya kesintisine yol açabilecek durumlar.
    - Seviye C: Şüpheli durumlar. Yukarıda tanımlı ilk iki seviyedeki duruma sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.

j) Her bir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin kuruma getireceği kayıplar ve bu riskler oluşmadan önce ve oluştuktan sonra hareket planları tanımlanmalı ve dokümante edilmelidir.
k) Acil durumlarda bilgi güvenliği yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle daha önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.
l) Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.
m) Olayın türü ve boyutuna göre emniyet veya diğer kurumlara başvurmak gerekebilir. Bu özel olaylar (hırsızlık vb), başvurulacak kurumlar, başvuru şekli (telefon, dilekçe vb), başvuruyu yapacak kurum yetkilisi önceden belirlenmiş ve dokümante edilmiş olmalıdır.

Yönetim Kurulu Başkanı