1. Amaç

Bu doküman, bilgi güvenliği ihlal olaylarının yönetiminin, tutarlı ve etkili bir şekilde uygulanmasını sağlamak için uyulması gerekli hususları belirlemek amacıyla oluşturulmuştur.

2. Kapsam

SDÜ0PL11 BGYS İhlal Olayı Yönetimi Politikası, SDÜ6GE01 BGYS Kapsamı dokümanında belirtilen tüm varlıkları ve tarafları kapsamaktadır.

3. Tanımlar

Kurum: Kütüphane ve Dokümantasyon Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. Uygulama

4.1 İhlal Olayı

İhlal olayı, Kurum'un iş süreçlerinin ve SDÜ6GE01 BGYS Kapsamı dokümanında belirtilen bilgi varlıklarının güvenliğini tehdit etme olasılığı olan, SDÜ0PL01 Bilgi Güvenliği Politikası ve ilgili politikalara aykırı tüm iç ve dış kaynaklı aksiyonlardır.

Bilgi güvenliği ihlal olayı örnekleri aşağıda listelenmiştir:

Fiziksel/Çevresel Güvenlik

- Yetkisiz personelin güvenli alanlarda bulunması
- Kurum dahilinde izinsiz fotoğraf/video kaydı yapılması
- Kritik BİDB tesislerinde enerji kesintisi, ortam koşullarının sınırlar dışına çıkması

Varlık Güvenliği

- Gizlilik içeren evrakın başıboş bırakılması
- Gizlilik içeren bilgi varlıklarının varlık sahibinden izinsiz olarak 3. Taraflarla paylaşılması

Sistem/Uygulama Güvenliği

- Antivirüs vb. korunma programları tarafından üretilen uyarı mesajları
- Kurum çapında, herhangi bir sistem ya da uygulamaya erişememe, performans kaybı
- İstemsiz olarak çalışan programlar ve istemsiz olarak açılan pencereler

Ağ/İletişim Güvenliği

- Ağ izleme sistemlerinin anormallik kayıtları üretmesi
- İnternet kesintisi

Teçhizat Güvenliği

- Cihaz kaybolması ya da çalınması
- Kurum dışına izinsiz olarak donanım çıkartılması
- Teçhizatın uygunsuz kullanımı

Fikri Mülkiyet Hakları

- Lisanssız yazılım kullanımı

Yasalara Uyum

- Bilgi varlıkları aracılığıyla T.C. Yasalarına uygunsuz davranışlar

4.2 Yaptırım

Kurum çalışanı kaynaklı ihlal olaylarında 657 Sayılı Devlet Memurları Kanunu hükümleri, tedarikçi ve hizmet sağlayıcı kaynaklı ihlal olaylarında hizmet sözleşmesi hükümleri esas alınır.

4.3 İhlal Olayını Belirleme ve Kanıt Toplama

Bilgi güvenliği ihlali, Kurum çalışanları ya da yükleniciler tarafından, farkına varıldığı anda SDÜ3FR09 BGYS İhlal Olayı Bildirimi Formu aracılığıyla BGYS Komisyonu Başkanı ya da BGYS Komisyonu üyelerine bildirilir.

Bilgi güvenliği ihlalinin etkisinin yüksek olabileceği şüphesi duyulan durumlarda, bildirim için yüz yüze görüşme ya da telefon gibi hızlı iletişim kanalları kullanılabilir. Bu tür durumlarda, form BGYS Komisyonu Başkanı tarafından hazırlanır.

İhlal olayının belirlenmesi sonrasında, olaya ilişkin kanıtlar toplanır. Hukuki kapsam dahilindeki disiplin işlemlerinin işletilmesi söz konusu ise, toplanacak kanıtların bilişim hukukuna uygun olmasına dikkat edilir.

Toplanan kayıtlar, yetkisiz erişime, silinmeye, bozulmaya ve değiştirilmeye karşı

korunur. İhlal olaylarına ilişkin kanıtlar en az 2 yıl süreyle saklanır.

4.4 Bilgi Güvenliği İhlal Olaylarını Değerlendirme ve Müdahale

İhlal olayına müdahalenin ilk hedefi, normal güvenlik seviyesinde çalışmanın sağlanması ve bu kapsamdaki gerekli kurtarma işlemlerinin başlatılmasıdır. İhlal olaylarında, olaya neden olan zafiyet en kısa sürede giderilir.

Müdahale için yeterli uzmanlık, yetkinlik, bilgi ve tecrübeye sahip olunmaması durumunda 3. Taraflardan destek alınır.

Etkisi çok yüksek olabilecek ihlal olaylarında, etkilenme potansiyeli olan sistemler kapatılır ya da diğer sistemlerden yalıtılır ve ilgili kişilerin tüm yetkileri askıya alınır.

İhlal olaylarından elde edilen veriler risk değerlendirmesinde girdi olarak kullanılır.

İhlal olayları sonrasında, olayın kök nedeni ve bir daha oluşmaması için gerekli önlemler belirlenerek uygulanır. Bu kapsamda alınabilecek önlem örnekleri aşağıda listelenmiştir:

- Bilgilendirme ya da farkındalık eğitim faaliyetleri düzenlenmesi
- Konuya ilişkin uzmanlık seviyesinin arttırılması ya da dış destek sağlanması
- Politika ve prosedürlerin gözden geçirilmesi, gerekliyse güncellenmesi
- Fiziksel/Çevresel kontrollerin gözden geçirilmesi, gerekliyse arttırılması
- Erişim yetkilerinin gözden geçirilmesi
- Zafiyet analizi yapılması, gerekliyse sızma testi yaptırılması
- Ağ kontrollerinin iyileştirilmesi
- Risk değerlendirmenin gözden geçirilmesi