OLAY İHLAL PROSEDÜRÜ

1. AMAÇ

Bu prosedürün amacı, Bilgi İşlem Daire Başkanlığı Bilgi Güvenliği Yönetim Sistemi kapsamında birimin sahibi olduğu bilgi varlıklarının bilerek veya bilmeyerek, kasten veya tesadüfen 3. şahısların eline geçmesi, kısmen veya tamamen durması / tahrip edilmesi durumunda ortaya çıkan olumsuz durumu yönetmek ve olası zayıflıkları tespit ederek, zayıflıkları kullanacak tehditlerin sonuçlarını ortadan kaldırmaktır.

1.1. İhlalin / Zayıflığın Ortaya Çıkması / Fark Edilmesi

1.1.1. İhlal olayını fark eden personel olayla ilgili olarak ivedilikle Bilgi İşlem Daire Başkanlığını haberdar eder ve **İhlal Olayı Formu** düzenler ve BGYS Temsilcisine iletir.

1.1.2. Olay zayıflık ise zayıflık kısmı, ihlal ise ihlal kısmı doldurulur ve **Olay İhlal Takip Çizelgesine** kaydedilir.

1.2. Araştırma

1.2.1. İhlal olayının fark edildiği tarih ve gerçekleştiği tarihin belirlenmesi ve olayla ilişkisi olabilecek unsurların ortaya çıkarılması aşamasıdır. İhlal olayı ile ilişkisi olabilecek unsurların belirlenmesi sonucunda ***Güvenlik Olayı Sınıflandırma Tablosuna*** göre **İhlal Olayı Formu** düzenlenir.

1.2.2. **Olay İhlal Takip Çizelgesi altı ayda bir** BGYS Temsilcisi tarafından gözden geçirilir. Yönetimin Gözden Geçirme Toplantısında sonuçlar raporlanır.

1.2.3. BGYS Temsilcisi, rapor çerçevesinde gerekli ihtiyaçları belirler (eğitim, araç, yazılım, donanım vs.) ve kaynakları ayırır.

1.3. Karar

1.3.1. Bu aşamada ihlalin ortaya çıkmasında sorumlu olan unsurlar hiçbir şüpheye yer vermeyecek şekilde ortaya konur ve karar verilir. Karar metni üç farklı içerikte hazırlanacaktır.

1.3.2. **İhlal: Personel**
İhlal personelden kaynaklanıyorsa disiplin yönetmeliğine göre hareket edilir. Bu durumda ihlalin kasıtlı veya bilmeyerek yapılıp yapılmadığı göz önünde bulundurulmalıdır.

1.3.3. **İhlal: Donanım /Yazılım**
İhlal bir yazılım veya donanımın hatasından kaynaklanıyor ise teknik rapor düzenlenerek BGYS Temsilcisine/Bilgi İşlem Daire Başkanına sunulur.

1.3.4. **İhlal: 3. Şahıslar**
İhlal 3. şahıslardan kaynaklanıyorsa gerekli tespitlerin yapılarak (ip no gibi) BGYS Temsilcisine raporlanır.

1.4. Güvenlik Olayı Sınıflandırma Tablosu

SEVİYE	TANIM	ÖNEM DERECESİ
1	Olay sonucunda, organizasyonun operasyonları için çok kritik olan faaliyetleri sürekliliği ciddi biçimde etkilenmektedir.	**Kritik**
2	Olay sonucunda bir uygulama veya sisteme yönelik kullanım etkilenmekte ve bu durum da organizasyonun faaliyetlerini etkilemektedir.	**Majör**
3	Olay sadece bir kullanıcı grubunu etkilemektedir. Kesintiye uğrayan faaliyetler organizasyonun operasyonlarını etkilememektedir.	**Minor**