LOGO Ornek Sirket	BG Olay ve Siber Olay Yönetimi Prosedürü	DOKÜMAN NO : YAYIN TARİHİ : REV. TARİHİ : VERSİYON NO :
	Hazırlayan : Onaylayan :	SAYFA NO :

Doküman Sorumlusu:	
İlk Yayın Tarihi:	
Versiyon No:	
Onay Tarihi:	
Onay Makamı:	
Gözden Geçirme Sıklığı:	
Gözden Geçirme Sorumlusu:	
Bir Sonraki Gözden Geçirme Tarihi:	

Versiyon	Tarih	Değişiklik Açıklaması

İçindekiler

LOGO Ornek Sirket	BG Olay ve Siber Olay Yönetimi Prosedürü	DOKÜMAN NO : YAYIN TARİHİ : REV. TARİHİ : VERSİYON NO :
	Hazırlayan : Onaylayan :	SAYFA NO :

1. GİRİŞ

1.1 Amaç

bilgi sistemleri altyapısında oluşabilecek güvenlik ihlallerinin zamanında tespit edilmesi, olaylara ilişkin aksiyon alınması, sebeplerinin analiz edilmesi ve kanıtların toplanması, sistemin en kısa sürede en az zarar ile tekrar çalışır duruma getirilmesi, olayların tekrar etmemesi konularında yönetim ve esaslar ile raporlanması konusundaki kuralları belirlemek amacıyla yayımlanmıştır.

1.2 Kapsam

Bilgi Güvenliği Olay Yönetimi Prosedürü tüm personeli, sözleşmeli personel, geçici personel ve kuruluş sistemlerine veya verilerine erişimi olan tedarikçi firmalar için geçerlidir. Bilgi güvenliği ihlal olayına yol açabilecek olası durumlar ve siber olaylar bu kapsamda ele alınmıştır.

1.3 İlgini Kanun ve Düzenlemeler

- Ödeme ve Elektronik para kuruluşlarının bilgi sistemleri ile ödeme hizmeti sağlayıcılarının ödeme hizmetleri alanındaki veri paylaşım servislerine ilişkin tebliğ,
- Olay yönetimi ve siber olaylar – Madde 7

1.4 Tanımlamalar ve Kısaltmalar

- BT (Bilgi Teknolojileri): Bilgi Teknolojileri
- İş Birimleri: Bilgi Teknolojileri birimi dışında kalan tüm grup ve birimler
- Kurum, Kuruluş:
- Tebliğ: Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ
- TCMB: Türkiye Cumhuriyet Merkez Bankası
- Üst Yönetim: yönetim kurulu üyeleri ile genel müdür ve genel müdür yardımcıları, İç Kontrol ve Risk Yönetimi ve Uyum Birimlerinin yöneticileri ile başka unvanlarla istihdam edilseler

dahi yetki ve görevleri itibarıyla Genel müdür yardımcısına denk veya daha üst konumlarda görev yapan yöneticileri

- Bilgi Güvenliği Olayı: bilgi sistemleri altyapısını etkileyen, çalışmasını engelleyen veya bünyesindeki verilerin bütünlüğünün, erişilebilirliğinin ve gizliliğinin olumsuz etkilenmesine sebep olan olaylar
- Bilgi Güvenliği Zayıflığı: Sunucu, bilgisayar ve çeşitli cihazların birbirlerine çeşitli yöntemlerle bağlanmasıyla oluşan yapıya verilen genel ad
- Denetim İzi (Log/İz Kaydı): Bir veri kaynağı hakkında zaman içindeki durumlarının ya da değişikliklerinin kayıt altına alınması sırasında oluşan sistemsel kayıtlar
- DoS (Denial of Service): Bir hedefe yönelik gerçekleştirilen, sistemin hizmet vermesini, kullanıcıların sisteme erişmesini engelleyen bir siber saldırı türü
- DDoS (Distributed Denial of Service): DoS saldırısının bir kaynaktan yerine birden fazla sayıda ve farklı kaynaktan başlatılmasıyla gerçekleşen olay