

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Kriz / Acil Durum Yönetimi Politikası	Doküman No	PLT-021
		İlk Yayın Tarihi	24.8.2023
		Revizyon Tarihi	24.8.2023
		Revizyon No	000
		Sayfa No	1 / 1

1. AMAÇ

Bu politika kurum çalışanlarının bilgi güvenliği ve iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dahilinde gerekli müdahaleyi yapabilmelerine yönelik standartları belirlemektedir.

2. KAPSAM

Bilgi güvenliğine yönelik tehlike durumlarında sisteme yapılacak direkt saldırılar, zararlı kod içeren programlar, kişilerin sisteme sızması, bilginin hırsızlığı, dışarıdan veya içeriden gerçekleştirilebilecek saldırıları kapsamaktadır.

3. SORUMLULUK

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanlığı sorumludur.

4. UYGULAMA

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

- Acil durum sorumluları atanmalıdır. Yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir.
- Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır.
- Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlaması için aynı ortamda kümeleme veya uzaktan kopyalama veya pasif sistem çözümlerini hayata geçirmelidir.
- Acil durumlarda sistem logları incelenmek üzere saklanmalıdır.
- Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.
- Yaşanan acil durumlar sonrası politikalar ve süreç yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
- Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
- Acil durumlarda Acil durum Müdahale ekibine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.
- İlgili yönetici tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.