KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI

1.0 AMAÇ

Bu politikanın amacı, ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ in çalışanlarının bilgi güvenliği ve iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dâhilinde gerekli müdahale yapabilmelerine yönelik standartları belirlemektir. 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 dâhilinde 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 POLİTİKA

a) Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir.

b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin uygulama veya veritabanı sunucularından donanım ve yazılıma ait problemler oluştuğunda yerel veya uzak sistemden yeniden kesintisiz çalışma sağlanabilmelidir.

c) Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlaması için aynı ortamda kümeleme veya uzaktan kopyalama veya pasif sistem çözümlerini hayata geçirilebilir. Kurumlar sistemlerini tasarlarken ne kadar süre iş kaybını tolere edeceklerini göz önüne almalıdırlar.

d) Acil durumlarda kurum içi işbirliği gerksinimleri tanımlanmalıdır.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI

e) Acil durumlarda sistem logları 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) 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.

k) Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgli makamlara iletilmelidir.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		