

BİLGİ GÜVENLİĞİ POLİTİKASI

Genel Çerçeve:

Şirketimiz, müşterilerine sunduğu hizmetler kapsamında aşağıdaki Bilgi Güvenliği Politikası ilkelerini benimsemiş ve uygulamaya koymuştur:

1. Gizlilik ve Mahremiyet Yönetimi

Personel ve müşterilere ait kişisel bilgilerin gizliliği ve mahremiyeti en üst düzeyde korunur.

2. Bilgi Bütünlüğü ve Erişilebilirlik

Bilginin doğruluğunu ve bütünlüğünü koruyacak, kesintisiz erişilebilirliğini güvence altına alacak teknik altyapı ve kontrol mekanizmaları oluşturulur.

3. Görev Ayrımı ve Onay Süreçleri

Tasarım, geliştirme, test ve uygulama aşamalarında görev ayrımı prensiplerine uygun yetkilendirme yapılır; kritik ve riskli işlemler için onay mekanizmaları devreye alınır.

4. Ortam Ayrımı

Geliştirme, test ve üretim ortamları fiziksel, mantıksal ve rasyonel açıdan birbirinden tamamen ayrıştırılır.

5. Minimum Yetki Prensibi

Kullanıcılara yalnızca görevlerini yerine getirmek için gerekli olan asgari yetkiler tanımlanır ve bu yetkiler düzenli aralıklarla gözden geçirilir.

6. Ağ Güvenliği

Dış kaynaklı tüm siber tehdit ve risklere karşı kapsamlı ağ güvenliği önlemleri hayata geçirilir.

7. Çok Katmanlı Güvenlik Duvarı

Çok katmanlı güvenlik duvarı sistemleri kurulur ve bu sistemler kesintisiz olarak izlenir.

8. Bilgi Varlıkları Yönetimi

Bilgi varlıklarının envanteri çıkarılır, sahipleri belirlenir ve bu varlıklar üzerindeki riskler sistematik olarak yönetilir.

9. Farkındalık ve Eğitim

Tüm personele bilgi güvenliği konusunda kapsamlı farkındalık eğitimleri verilir ve çalışanların aktif katılımı sağlanır.

10. Politika ve Mevzuata Uyum

Personelin belirlenmiş bilgi güvenliği politikalarına, prosedürlerine ve yasal düzenlemelere uyumu yazılı taahhütlerle zorunlu kılınır.

11. İş Sürekliliği Yönetimi

İş süreçlerinde oluşabilecek kesintilerin engellenmesi ve bilgiye kesintisiz erişimin sağlanması amacıyla iş sürekliliği planları geliştirilir ve uygulanır.

12. Erişim Kontrolü

Yetkisiz erişimlerin önlenmesi için tüm kritik alanlarda kapsamlı güvenlik kontrolleri ve erişim denetim mekanizmaları uygulanır.

13. Şifre ve Anahtar Güvenliği

Kullanılan tüm şifre ve güvenlik anahtarlarının güvenilirliği ve karmaşıklığı garanti altına alınır.

14. Fiziksel ve Çevresel Güvenlik

Bilginin işlendiği ve saklandığı tüm fiziksel alanlarda gerekli güvenlik ve çevre koruma önlemleri alınır.

15. Operasyonel Güvenlik

Bilgi sistemlerinin işletilmesinde gerekli tüm güvenlik kontrolleri uygulanır, ilgili rol ve sorumluluklar net olarak tanımlanır.

16. Güvenlik Organizasyonu

Bilgi güvenliği faaliyetlerinin koordinasyonu, yönetimi ve sürdürülmesi için ayrı bir organizasyon yapısı oluşturulur.

17. Veri Koruma Önlemleri

Kişisel veriler ve hassas ödeme bilgilerinin iletimi ve saklanmasıda şifreleme, maskeleye gibi ileri düzey güvenlik önlemleri uygulanır.

18. Sistem Geliştirme Güvenliğı

Bilgi sistemlerinin edinimi, geliştirilmesi ve bakımında güvenlik gereksinimleri belirlenir ve sistematik olarak uygulanır.

19. Olay Yönetimi

Bilgi güvenliğı olaylarının tespit edilmesi, raporlanması ve tekrarının önlenmesi için etkin bir olay yönetimi süreci işletilir.

20. Sürekli İyileştirme

Bilgi güvenliğı yönetim sisteminde sürekli gelişim ve iyileştirme çalışmaları yürütölmesi taahhüt edilir.