ODİNE SOLUTİONS TEKNOLOJİ TİCARET VE SANAYİ A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

Şirketimiz **Odine Solutions Teknoloji Ticaret Ve Sanayi A.Ş. ("Şirket")** Bilgi Güvenliği Politikasının amacı, tabi olduğu tüm mevzuat, standart ve sözleşme gereksinimleri çerçevesinde; Şirket bilgi sistemlerinin ve bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin sağlanması amacıyla ihtiyaç duyulan faaliyetleri tanımlamaktır.

Bilgi Güvenliği Politikası, bilgileri ve iş sistemlerini kullanan tüm çalışanlar için coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve uygulanması zorunludur.

Bu çerçevede;

Bilgi Güvenliğinin Sağlanması

- Tüm bilgilerin doğru ve tam olmasını sağlamak, bilgi hatalarını ve eksikliklerini minimize etmek için sürekli kontroller yapmayı.

- Bilgilerin gizliliğini korumak ve yetkisiz erişimlere karşı etkili güvenlik önlemleri almak. Bilgilere sadece yetkili kişilerin erişimini sağlamayı.

- Bilgilerin bütünlüğünü ve sürdürülebilirliğini sağlamak için veri yedekleme, güvenli depolama ve bilgi yaşam döngüsü yönetimi uygulamalarını etkin şekilde kullanmayı.

- Bilgilerin gerekli durumlarda ve sadece yetkili kişiler tarafından erişilebilir olmasını temin etmeyi.

Bilgi Güvenliği Risk Yönetimi

- Bilgi güvenliğine yönelik riskleri sistematik olarak belirlemek, değerlendirmek ve yönetmeyi.

- Belirlenen riskleri kabul edilebilir seviyelere indirmek için risk değerlendirme ve risk yönetimi süreçlerini kullanarak sürekli iyileştirme süreçleri yürütmeyi.

- Etkin bir bilgi güvenliği risk yönetimi yaklaşımı oluşturarak, potansiyel tehdit ve zafiyetleri önceden belirlemek ve bunlara karşı uygun önlemler almayı.

Kaynakların Tahsisi ve Yetki Dağılımı

- Bilgi güvenliği risklerinin yönetimi ve güvenlik kontrollerinin etkin bir şekilde işletilmesi için yeterli insan kaynağı, teknoloji ve finansal kaynaklar ayırmayı.

- Bilgi güvenliği yönetimi için gerekli yetki ve sorumlulukları açıkça tanımlamak ve uygun kişilere bu yetki ve sorumlulukları vermeyi.

İş Sürekliliği ve İhlal Yönetimi

- İş etki analizlerini gerçekleştirmeyi.

- Olası kesintiler ve acil durumlar için iş sürekliliği planları geliştirmek, bu planları düzenli olarak test etmeyi.

- Bilgi güvenliği ihlallerini etkin bir şekilde yönetmek için gerekli sistemleri kurmak ve ihlallerin tekrarını önlemek amacıyla uygun düzeltici ve önleyici önlemler almayı.

Servis Yönetimi

- Bilgi güvenliği politikaları doğrultusunda sunulan hizmetlerin kalitesini sürekli olarak izlemeyi ve iyileştirmeyi.

- Müşterilere taahhüt edilen hizmet seviyelerini belirlemek, izlemek ve bu seviyelere uygun hizmet sunmayı.

- Bilgi güvenliği prensiplerine uygun olarak servis sürekliliğini sağlamak, servis kesintilerini minimize etmek ve acil durumlar için yedekleme ve kurtarma planları oluşturmayı.

- Hizmetlerin güvenli bir şekilde sunulması için gerekli prosedürleri oluşturmak, bu prosedürlerin etkinliğini düzenli olarak değerlendirmeyi ve güncellemeyi.

- Müşterilerin bilgi güvenliği ile ilgili geri bildirimlerini dikkate alarak, servis yönetim süreçlerinde iyileştirmeler yapmayı.

Mevzuat ve Sözleşmelere Uyum

- Mevzuattan kaynaklanan tüm bilgi güvenliği gereksinimlerini izlemek, anlamak ve yerine getirmeyi.

- İş ortakları, müşteriler ve tedarikçilerle yapılan sözleşmelerde yer alan bilgi güvenliği hükümlerini takip etmeyi ve bu hükümlere uyumu sağlamayı.

Güncel İş Plan ve Prosedürler

- İş planları ve prosedürlerinin güncel, uygulanabilir ve etkin olmasını sağlamak için düzenli olarak gözden geçirmeyi ve gerekli güncellemeleri yapmayı.

Güvenli İş Ortamı

- İç ve dış paydaşlarla güvenli bir iş ortamı oluşturmak için bilgi güvenliği farkındalığını artırmayı.

- Fiziksel ve dijital güvenlik önlemleri alarak iş ortamında güvenliği sağlamayı.

Bilgi Güvenliği Eğitimi

- Tüm çalışanlara bilgi güvenliği ve siber güvenlik eğitimi sunmayı, bilgi güvenliği konusunda bilinç ve farkındalıklarını artırmayı.

- Üçüncü taraflar ve paydaşlar için bilgi güvenliği farkındalığını artırmak üzere gerekli eğitimler ve bilgilendirmeler yapmayı.

Denetimler ve Uyum

- Tabi olunan tüm mevzuat, standart ve sözleşme gereksinimlerine uyumu sağlamak amacıyla düzenli iç ve dış denetimler gerçekleştirmeyi.

- Denetimler sonucunda ortaya çıkabilecek uygunsuzlukları gidermek için planlanan faaliyetleri desteklemek ve takip etmeyi.

Sürekli İyileştirme

- Bilgi güvenliğine yönelik sürekli iyileştirme çalışmaları yapmak, yeni tehdit ve zafiyetlere karşı önlemler geliştirmeyi.

- Çalışanların katılımı ile Entegre Yönetim Sistemini sürekli iyileştirmek ve güncel tutmayı

Amaç olarak edinmiş bulunmaktayız.

Şirket, bilgi güvenliği kapsamında; bilgi güvenliği politikasını ve destekleyici prosedürleri hazırlar ve uygulamasını gözetir ve bu politika ile ilgili faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar.

İşbu Bilgi Güvenliği Politikası 22/07/2024 tarih ve 2024/15 sayılı Yönetim Kurulu kararı ile yürürlüğe girmiş olup, ayrıca Şirket kurumsal internet sitesi üzerinden kamuya açıklanır. Bilgi Güvenliği Politikasında yapılacak değişiklikler de aynı usule tabiidir.