İş Net Elektronik Bilgi Üretim Dağıtım Ticaret ve İletişim Hizmetleri A.Ş. (İşNet); bilgi güvenliğinin etkin yönetimi için ISO/IEC 27001 standardına uyumlu Bilgi Güvenliği Yönetim Sistemi'ni işletmektedir. İlgili mevzuat ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardı kapsamında, sunduğu hizmetlerin sorunsuz bir şekilde yürütülebilmesi için bilgi güvenliğini, temel ilkelerinden biri haline getirmiş olup sahip olduğu bilgi varlıklarının kritiklik derecesini göz önünde bulundurarak Bilgi ve İletişim Güvenliği Rehberi'nde yer alan uyum sürecini işletmekte ve gerekli tedbirleri uygulamaktadır. Bu Politika İşNet'in tüm faaliyetlerini ve bilgi varlıklarını kapsamaktadır.

Bu çerçevede; İşNet'e ait bilgi varlıklarının ve tüm faaliyetlere ilişkin bilgilerin sistemli bir şekilde yönetilmesi ve korunması gerektiğinin bilincinde bir kurum olarak Bilgi Güvenliğinin temel esasları olan Gizlilik, Bütünlük ve Kullanılabilirlik parametrelerinin İşNet'te yer alan tüm bilgi ve bilgi varlıklarında tesis edilmesini sağlamak amacıyla aşağıdaki politikalara uymayı beyan ve taahhüt ederiz.

- İşNet'in ve müşterilerinin marka itibarını, güvenilirliğini ve imajını korumak,
- İlgili taraf ve paydaşların bilgi güvenliği ihtiyaç ve beklentilerini karşılamak,
- Bilgi güvenliği kapsamında uymakla yükümlü olduğumuz yasal mevzuat ve sözleşmelerden doğan/doğabilecek şartlara uygun hareket etmek,
- Bilgi güvenliği kapsamında İşNet bünyesinde ilgili kişileri atamak, görev, sorumluluk ve yetkilerini belirlemek,
- Bilginin gizlilik, bütünlük ve erişilebilirlik etkilerini değerlendirilerek sınıflandırmasını yapmak,
- İşNet'in çalışanların, müşterilerin, tedarikçilerin ve diğer tüm paydaşların bilgi güvenliğini sağlamak amacıyla gizliliği koruyacak güvenlik önlemlerini almak,
- Paydaşların bilgilerinin yetkisiz erişim, ifşa, değiştirme veya kayıptan korunması için gerekli süreçler ve kontroller uygulamak,
- İşNet'in stratejik yönü ile uyumlu bilgi güvenliği hedefleri belirlemek ve uygulamak,
- Bilgi ve bilgi varlıklarını koruyacak yapıları kurmak, gerekli güvenlik önlemlerini almak, ilgili politikaları oluşturmak, uygulamak ve sürekli iyileştirme çalışmalarını yapmak,
- Bilgi güvenliğini etkileyebilecek riskleri analiz etmek, güvenlik kontrollerinin sağlıklı bir şekilde işletilmesi için sorumluları belirlemek ve riskleri kabul edilebilir seviyeye indirebilmek için aksiyonlar almak,
- İşNet'in bilgi güvenliği faaliyetlerinin verimli bir şekilde çalışması için gerekli olan kaynakları tahsis etmek,

- Bilgi güvenliği yönetim sistemi gerekliliklerinin İşNet'in süreçlerine entegrasyonu sağlamak,
- Bilgi güvenliği yönetim sistemi konusundaki sürekli iyileştirme ve geliştirmeyi desteklemek için tüm çalışanların farkındalıklarının artırılması amacıyla eğitimler vermek,
- Bilgi güvenliğinin etkinliğinin ölçümü için periyodik gözden geçirme çalışmaları gerçekleştirmek, gerekli düzeltici ve iyileştirici faaliyet çalışmalarını yürütmek ve düzenli iç ve dış denetimlerle değerlendirmek,
- Bilgi Güvenliği Yönetim Sistemi'nin işletilmesi ve sürekliliğinin sağlanması için gereken kontrollerin tesis edilmesini ve gözetimini bu politikaya bağlı alt politikalar, prosedürler ve talimatlar vasıtasıyla sağlamak,
- Tedarikçiler ve dış hizmet sağlayıcılarla olan ilişkilerde bilgi güvenliği gerekliliklerini sağlamak için uygun kontrol faaliyetleri gerçekleştirmek,
- Bilgi güvenliği olaylarının hızlı ve etkili bir şekilde ele alınması için etkin bir olay yönetim süreci yürütmek.