GÖÇTUR TURİZM BİLGİ GÜVENLİĞİ POLİTİKASI

Göçtur Turizm Üst Yönetimi olarak;

Bilgiyi etkin ve güvenli bir şekilde günümüz teknolojilerine uygun, geliştirilebilir ve birbiri ile entegre olarak kişilere bağlı olmayan bir sistem içinde çalışmasını ve şirket bilgileri gizliliği ilkesi ile sürdürülmesini sağlayarak verileri tüm paydaşlarımızın mutluluğu ve güvenliği göz önüne alınarak etik kurallara uygun olarak yürütmek ve yönetmekteyiz.

İşletmelerimizdeki bütün bilgi varlıklarını korumak üzere yürüttüğümüz bilgi güvenliğini sürekli iyileştirmek ve geliştirmek amacıyla;

- Bilgi güvenliğini kurumsal bir sorumluluk olarak ele alır, bilgi güvenliği risklerinin yönetimi ve güvenlik kontrollerinin sağlıklı bir şekilde işletilmesi için gerekli kaynakları ayırır, yetki ve sorumluları belirleriz,
- Çalışanlarımızın, üçüncü taraf ve paydaşlarımızın bilgi güvenliğine yönelik rol ve sorumlulukları hakkında farkındalığını arttırmak üzere düzenli eğitim aktiviteleri düzenleriz,
- Kurumsal bilgilerimiz yanında; müşterilerimizin, çalışanlarımızın ve tüm iş ortaklarımızın bilgilerinin güvenliği için ilgili tüm yasa ve sözleşmelerden kaynaklanan gereksinimlere uyumu, tüm çalışanlarımızın birincil sorumluluğu olarak kabul ederiz
- Bilgi güvenliği kapsamı dâhilindeki bilginin gizlilik, bütünlük ve erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi için bilgi güvenliği risk değerlendirme sürecinin uygulanmasını ve risk sahiplerini belirlemeyi,
- Bilgi güvenliği kapsamı dâhilindeki bilginin gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik bir çerçeveyi tanımlamayı,
- Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmeyi,
- Tabi olduğumuz ulusal veya sektörel düzenlemelerde, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklardan kaynaklanan bilgi güvenliği gereksinimlerini sağlamayı,
- Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmayı ve sürekliliğe katkıda bulunmayı,
- Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmayı,
- Etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumayı ve sürekli iyileştirmeyi,
- Kurum itibarını geliştirmeyi, bilgi güvenliği temelli olumsuz etkilerden korumayı,
- Bilgi güvenliği kapsamında gizlilik açısından farklı seviyelerde hassasiyete sahip bilgiler hakkında kurumsal farkındalığı artırmayı, farklı hassasiyet seviyelerine sahip bilgiler için uygulanması önerilen mantıksal, fiziksel ve idari kontrolleri belirlemeyi ve taşınabilir ortamlarda bulunan verilerin saklanma ve imha kurallarını tanımlamayı,

Taahhüt ederiz.