BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI -BİLDİRİSİ

INFORMATION SECURITY MANAGEMENT SYSTEM POLICY STATEMENT

Bilgi Güvenliği Yönetim Sistemi politikamız ile yürüttüğümüz tüm çalışmalar, aşağıdaki temel prensipler doğrultusunda şekillenmektedir.

- Kendisi ve paydaşlarının bilgi varlıklarına güvenli bir şekilde erişim sağlamayı,
- Bilginin kullanılabilirliğini, bütünlüğünü ve gizliliğini korumayı,
- Kendisinin ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi,
- Kurumun güvenilirliğini ve marka imajını korumayı
- Bilgi güvenliği ihlali durumunda gerekli görülen yaptırımları uygulamayı,
- Tabi olduğu ulusal, uluslararası veya sektörel düzenlemelerden, ilgili mevzuat ve standart gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklardan kaynaklanan bilgi güvenliği gereksinimleri sağlamayı,
- İş/Hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmayı ve işin sürekliliği ve sürdürülebilirliğini sağlamayı,
- Kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumayı ve iyileştirmeyi,
- Bilgi güvenliği farkındalığını arttırmak amacıyla yetkinlikleri geliştirecek eğitimleri sağlamayı,

Taahhüt ederiz.

All the work we carry out with our Information Security Management System policy is shaped in line with the following basic principles.

- To provide secure access to the information assets of itself and its stakeholders,
- To protect the availability, integrity and confidentiality of information,
- To evaluate and manage the risks that may occur on the information assets of itself and its stakeholders,
- To protect the reliability and brand image of the institution
- To apply the necessary sanctions in case of information security breach,
- To meet information security requirements arising from national, international or sectoral regulations to which it is subject, to fulfill the requirements of the relevant legislation and standards, to meet its obligations arising from agreements, and corporate responsibilities towards internal and external stakeholders,
- To reduce the impact of information security threats on business/service continuity and to ensure business continuity and sustainability,
- To maintain and improve the level of information security with the established control infrastructure,
- To provide trainings that will develop competencies in order to increase information security awareness,

We commit.