Information Security Policy

1. To manage our information assets, to assess the security values, needs and risks of the assets, to develop and implement control mechanisms against security risks.
2. To define the framework and evaluate the effects of threats on our assets' confidentiality, integrity and accessibility and to keep track of current risks in accordance to the continuous development cycle.
3. To meet the requirements of national or industry-specific regulations, legal legislations, fulfill the obligations of agreements, to meet the information security requirements that exist due to corporate responsibility towards internal and external stakeholders.
4. To decrease the effects of information security threats on our business / service continuity.
5. To have adequate competency to respond to information security cases fast and effectively, and the ability to minimize the effects.
6. To enhance our corporate reputation, to protect our corporation from the negative effects that can result from information security leaks.
7. To raise information security awareness among our employees.

Bilgi Güvenliği Politikası

1. Bilgi varlıklarımızı yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek ve uygulamak.
2. Tehditlerin varlıklarımız üzerindeki gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik çerçeveyi tanımlamak ve bu çerçeve uyarınca sürekli gelişim döngüsüne uygun şekilde güncel riskleri sürekli takip etmek.
3. Tabi olduğu ulusal veya sektörel düzenlemelerden, ilgili yasal mevzuatın gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülükleri karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından ortaya çıkan bilgi güvenliği gereksinimlerini sağlamak.
4. İş / hizmet sürekliliğimiz üzerinde bilgi güvenliği tehditlerinin etkisini azaltmak.
5. Gerçekleşebilecek bilgi güvenliği olaylarına, etkin ve hızlı müdahale edebilecek ve olayların etkilerini minimize edecek yetkinliğe sahip olmayı temin etmek.
6. Kurum itibarımızı geliştirmek; kuruluşumuzu, bilgi güvenliği kırılmalarından kaynaklanabilecek olumsuz etkilerden korumak.
7. Çalışanların bilgi güvenliğini farkındalığını geliştirmek.