BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ
POLİTİKASI

TS EN ISO 27001:2017 Bilgi Güvenliği Yönetim Sistemin ana teması; ***BNB MÜHENDİSLİK SUNMUŞ OLDUĞU HİZMET VE ÜRETİMİ KAPSAMINDA*** bilgi güvenliği yönetiminin sağlandığını göstermek, risk yönetimini güvence altına almak, bilgi güvenliği yönetimi süreç performansını ölçmek ve bilgi güvenliği ile ilgili konularda üçüncü taraflarla olan ilişkilerin düzenlenmesini sağlamaktır.

Bu doğrultuda ***BGYS Politikamızın*** amacı;

- İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı ***BNB MÜHENDİSLİK*** in bilgi varlıklarını korumak, iş proseslerinin gerektirdiği şekilde bilgiye erişebilirliği sağlamak, yasal mevzuat şartlarını karşılamak,
- Yürütülen tüm faaliyetlerde Bilgi Güvenliği Yönetim Sisteminin üç temel öğesinin sürekliliğini sağlamak.

  Gizlilik: Önem taşıyan bilgilere yetkisiz erişimlerin önlenmesi,

  Bütünlük: Bilginin doğruluk ve bütünlüğünün sağlandığının gösterilmesi,

  Erişebilirlik: Yetkisi olanların gerektiği hallerde bilgiye ulaşılabilirliğinin gösterilmesi,
- Bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek ve uygulamak
- Bilgi varlıkları, değerleri, güvenlik ihtiyaçları, zafiyetleri, varlıklara yönelik tehditlerin, tehditlerin sıklıklarının saptanması için yöntemlerin belirleyeceği çerçeveyi tanımlamak.
- Tehditlerin varlıklar üzerindeki gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik bir çerçeveyi tanımlamak.
- Risklerin işlenmesi için çalışma esaslarını ortaya koymak.
- Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmek
- Tabi olduğu ulusal veya uluslararası düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.
- Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak
- Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmak
- Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek.
- Kurum itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak
- Bilgi Güvenliği Yönetim Sisteminin sürekliliğini sağlamak
- Bilgi Güvenliği Yönetim Sistemini sürekli iyileştirmek

Genel Müdür