

BGYS POLİTİKASI

Doküman No : BGEK-02

Yayın Tarihi : 01.08.2018

Revizyon No / Tarihi : 00/-

Sayfa Sayısı : 2

REVİZYON TABLOSU

| REVİZYON NO | REVİZYON GEREKÇESİ | TARİH |
|-------------|--------------------|-------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

HAZIRLAYAN

BGYS KOORİNATÖRÜ

ONAYLAYAN

GENEL MÜDÜR

| | | | |
|---|------------------------|-----------------------------------|-----------------------------|
|  | BGYS POLİTİKASI | | |
| | BGEK-02 | YAYIN TARİHİ 01.08.2018 | REVİZYON NO/TARİHİ 02 |

TS EN ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemin ana teması " Bilgi Güvenliği Faaliyetleri" kapsamında; insan, alt yapı, yazılım, donanım, kuruluş bilgileri, üçüncü şahıslara ait bilgiler ve finansal kaynaklar içerisinde 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;

- *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*

| | |
|--------------------------|-------------------------|
| <u>HAZIRLAYAN</u> | <u>ONAYLAYAN</u> |
| BGYS KOORİNATÖRÜ | GENEL MÜDÜR |