Siber ve Bilgi Teknolojileri Güvenliği'nin sağlanmasına yönelik olarak yürütülecek çalışmalarda esas alınması gereken temel ilkeler şunlardır:

- Uluslararası sözleşmelerle teminat altına alınmış temel insan hak ve hürriyetlerinin korunması,
- Alınacak tedbirlerin Ölçülülük İlkesine göre belirlenmesi,
- Karar alma süreçlerine tüm paydaşların katılımını sağlayacak kapsayıcı bir yaklaşımın benimsenmesi,
- Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile ele alan bütüncül bir yaklaşımın benimsenmesi,
- Geliştirilecek çözümlerde güvenlik ile kullanılabilirlik arasında denge kurulması,
- Ulusal mevzuatların göz önünde bulundurulması ve mümkün olabildiğince uyumluluğun sağlanması,
- Siber ve Bilgi Teknolojileri Politikası kapsamında stratejilerin geliştirilmesi ve etkin bir şekilde uygulanması,
- Mevcut güvenlik yasalarına göre siber ortamlarda gereken çalışmaların yapılması,
- Bilgi işlem sistemlerini (BİS) hedef alan saldırıların önlenmesi, tespit edilmesi, bunlara müdahale edilmesi ve en az hasarla geri dönüşün sağlanması için gereken çalışmaların yapılması,
- Siber güvenlik kültürünün benimsenmesinin sağlanması,
- Temel paydaşların belirlenmesi,
- Siber güvenlik programının denetlenmesi, değerlendirilmesi, doğrulanması ve etkinliğinin arttırılması,
- İnternet kullanıcılarının kişisel mahremiyet ve siber ortamdaki kimliğin sınırları hakkında eğitilmesi,
- Teknik ve işlevsel tedbirlerin alınması,
- Kurumsal yapılanmanın oluşturulması,
- Kapasitenin geliştirilmesi ve farkındalığın arttırılması,
- Siber ortamda koruma ve gözetme yetkilerinin belirlenmesi,
- Teknik ve işlevsel tedbirlerin alınması,
- Güvenliği kanıtlanmış standartların ve teknik çözümlerin kullanılması,
- Siber güvenlik olaylarının güvenilir şekilde raporlanması,
- Gerçekçi ve uygulanabilir acil durum yönetimi planları hazırlanması,
- Daha sağlam ve dinamik şifreler, çok parametreli kimlik doğrulama, denetim ve cihaz kimlik doğrulaması ile desteklenen kullanıcı kimlik doğrulaması uygulanması,
- Tekrarlanan istemler gönderen blok cihazların tespiti ve bunlardan gelen istemlerin reddedilmesi,

- Anti-virüs ve anti-spyware sistemlerinin düzenli olarak güncellenmesi, yetkisiz konfigürasyon değişikliklerine duyarlı donanım sistemlerinin kullanılması,
- Güvenlik duvarı ve dıştan içe saldırı tespit sistemleri kullanılması, sistemlerin sürekli izlenmesi ve denetlenmesi, sistemlerin sadece belli güvenlik düzeyine sahip olan kısımlarının İnternete açılması,
- Yeni teknolojilere ilişkin yeterli düzeyde kullanıcı eğitimi verilmesi,
- Farklı güvenlik seviyelerine sahip Bilgi İşlem Sistemleri arasındaki farkın kapatılması,
- Şebekelerde veya sistemlerde bulunan açıklıkların kamuoyuna açıklanması, incelenmesi ve iyileştirilmesi esnasında belli bir sorumluluk bilinci ve etik anlayışı içinde hareket edilmesi,
- Güvenlik çözümleri üreticileri ile iş birliği içinde çalışılması,
- Siber tehditlerle mücadele için etkin kurumsal yapıların oluşturulması ve konuyla ilgili mevcut ve yeni girişimler arasında koordinasyon sağlanması,
- Siber güvenlik girişimleri için önceliklerin belirlenmesi,
- Bilgi ve iletişim altyapılarının ve hizmetlerinin geliştirilmesi amacıyla ISO 27001 kapsamında süreçlerin sertifikalandırılması,
- Bilgisayar ve şebeke güvenliğini izleyen ve siber saldırı mağdurlarına olaylara müdahale etmeyi sağlamak amacıyla aşağıdaki çalışmalar takip edilecektir:
  - Reaktif yöntemler (uyarma, saldırılara müdahale, saldırı analizi, açıklıklarla mücadele, açıklık analizi ve koordinasyon),
  - Proaktif yöntemler (bilgilendirme, teknolojiyi izleme, güvenlik denetimi ve değerlendirme, güvenlik yönetimi, güvenlik araçları geliştirme, saldırı tespit hizmetleri),
  - Güvenlik kalite yönetim sistemleri (risk analizi, kriz yönetimi, farkındalık oluşturma, eğitim verme, ürün veya belgelerin değerlendirilmesi)
- Yetki alanlarına giren bilgisayar güvenlik olaylarının engellenmesi veya çözülmeye çalışılması,
- Tüm paydaşlar ile güvenilir ilişkiler kurarak saldırı ve açıklıkları izleme, tespit etme ve analiz etme aşamalarında onlarla birlikte etkin şekilde çalışılması,
- Tüm paydaşların siber tehditler konusunda uyarılması, siber saldırılara maruz kalan paydaşlara saldırı tespitinden çözümüne kadar gereken desteğin sağlanması.

Siber ve Bilgi Teknolojileri Güvenlik Politikası kapsamında yukarıda açıklanan çalışma ilkelerine uyum sağlanacağı taahhüt edilmektedir.

REVİZYON BİLGİLERİ

Revizyon No	Revizyon Tarihi	Revizyon Açıklaması
0	-	İlk yayın.

HAZIRLAYAN	ONAYLAYAN
Kalite Yönetim Sistemleri	Mehmet ATEŞ Genel Müdür

İmzalıdır.