Revizyon İzleme Tablosu		
Rev. No	**Rev. Tarihi**	**Açıklama**
00	-	İlk Yayın

1. AMAÇ

Bu politikanın amacı kurum bünyesinde kullanılan internet erişimi hakkında bilgi güvenliği açısından standart oluşturmaktır. İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır.

2. SORUMLULUKLAR

Bu politikanın uygulanmasından kurum ağları veya iletişim kanalları üzerinden internet erişimi sağlayan herkes sorumludur.

3. UYGULAMA

- Bütün kullanıcılar ve Sistem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkmamalıdır.
- Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkacaktır. Ağ güvenlik duvarı kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır. Ağın dışından ağın içine erişimin denetimi burada yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmelidir.
- İhtiyaçlar doğrultusunda içerik filtreleme sistemleri kullanılabilir. İstenmeyen siteler (kumar, şiddet vs.) Checkpoint aracılığıyla engellenebilir.
- Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme sistemleri kullanılmalıdır(Checkpoint, IPS, vb.). Şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. Checkpoint, şüpheli durumlarda loglama işlemi yapar ve sistem yöneticileri düzenli aralıklarla bu logları izler. Checkpoint saldırı tespit ettiği durumlarda ise saldırı kaynağını bloklayarak olası tehtidleri önler.
- Anti-virüs gateway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik virüslere karşı taranmalıdır.
- Ancak yetkilendirilmiş sistem yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahiptir. Çalışılan projeler dahilinde ftp ve telnet yetkisi ilgili personellere verilebilmektedir.
- Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemelidir. İndirilecek dosyalara virüs taraması yapılacağı için zararlı içerikler anti-virüs uygulaması tarafından engellenecektir.
- Üçüncü şahısların kurum internetini kullanmaları bilgi işlem sorumlularının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.