1. **AMAÇ – KAPSAM:**

İnternetin amaç dışı kullanımını engellemek, etiğe ve yasalara uygun kullanımını sağlamak, gerek firmamızın ve gerekse hizmet verdiğimiz kurumların güvenli internet erişimine sahip olması için standartları belirlemektir.

1. **SORUMLULAR:**

Bu prosedürün oluşturulmasından Bilgi İşlem sorumlu olup bütün bilgisayar kullanıcıları uygulamadan sorumludur.

1. **UYGULAMA:**

**Genel Kurallar:**

Bütün kullanıcılar ve sistem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkmamalıdır.

1. Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkmalıdır. Ağ güvenlik duvarı (firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet 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.
2. Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografik, oyun, kumar, şiddet içeren vs) yasaklanabilmelidir.
3. Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır. (Intrusion Detection an Prevention Systems-IPS): Şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IPS, şüpheli durumlarda e-posta veya SMS gibi yöntemlerle sistem yöneticisini uyarabilmektedir.
4. Anti-virus gateway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik (smtp, pop3, ayrıca mümkünse http ve ftp vs) virüslere karşı taranmalıdır.
5. Kurumlar internet erişimlerinde firewall, anti-virus, içerik kontrol vs. güvenlik kriterlerini hayata geçirmelidirler.
6. Ancak yetkilendirilmiş Sistem Yöneticileri ve Genel Müdür internete çıkarken bütün servisleri kullanma hakkına sahiptir. Bunlar; www,ftp,telnet, ping, traceroute vs.
7. Hiçbir kullanıcı peer-to-peer bağlantı yoluyla internetteki servisleri kullanamayacaktır. (Örnek; KaZaA, iMesh, eDonkey2000, Gnutella, Napster, Aimster, Madster, FastTrack, Audiogalaxy, MFTP, eMule, Overnet, NeoModus, Direct Connect, Acquisition, BearShare, Gnucleus, GTK-Gnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, XoLoX, OpenNap, WinMX. v.b.)
8. Bilgisayarlar arası ağ üzerinden ICQ, MIRC, Messenger, Gtalk v.b. mesajlaşma ve sohbet programları gibi chat programları kullanılmamalıdır. Anlık Mesajlaşma için kurum içi anlık mesajlaşma uygulaması kullanılmalıdır. Hiçbir kullanıcı internet üzerinden Multimedia Streaming yapmamalıdır.
9. Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.
10. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirilmemelidir.
11. İş ile ilgili olmayan (müzik, video dosyaları ) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek yasaktır.
12. İnternet üzerinden firma tarafından onaylanmamış yazılımlar indirilemez ve bilişim sistemleri üzerine bu yazılımlar kurulamaz. İşe yönelik yazılım ihtiyaçları için ilgili prosedürler dahilinde ilgili birim amirine müracaat edilmesi gerekmektedir.
13. Üçüncü şahısların firma internetini kullanmamalıdır. Fakat ihtiyaç halinde sınırlı kalmak koşuluyla ilgili yönetici tarafından geçici olarak verilebilir.
14. **İLGİLİ DOKÜMANLAR**