1. Amaç

Bu politikanın amacı, "KTÜN bünyesinde kullanılan veya uzak bağlantı yöntemleriyle KTÜN ağına bağlanan" bilgisayarlar ve kötücül yazılımların tehdidinde olan tüm sistemlere yönelik antivirüs güvenlik yazılımı kullanımı ve uygulamaların güvenilir kanallardan edinilmesi esaslarının tanımlanmasıdır.

2. Kapsam

"KTÜN bünyesinde kullanılan veya uzak bağlantı yöntemleriyle KTÜN ağına bağlanan" tüm bilgisayarlar, kötücül yazılımların tehdidinde olan tüm sistemler ve bunları kullanan tüm kullanıcılar bu politika kapsamındadır.

3. Sorumlular

Bu politikanın oluşturulmasından BGYS Komisyonu sorumludur. Uygulanmasından tüm kullanıcılar sorumludur.

4. Tanımlar

Politika maddeleri anlatılırken "Kuruma ait olsun veya olmasın kurum ağına bağlanan veya kurum işleri için kullanılan" bilgisayarlar ve kötücül yazılımların tehdidinde olan tüm sistemler(sunucu, tablet, dizüstü, akıllı telefon vb.) için genel olarak "cihaz" ifadesi kullanılacaktır.

5. Uygulamalar

- Tüm cihazlarda antivirüs yazılımı yüklü ve güncel olmalıdır.
- Antivirüs yazılımları gerçek zamanlı (real time) koruma sağlayacak şekilde konfigüre edilmelidir.
- Antivirüs yazılımı ve virüs tanımları otomatik olarak güncellenmelidir.
- Virüs bulaşan cihazlar yayılma durumuna karşı kesinlikle kurum ortak ağından çıkarılmalı tam olarak temizleninceye kadar ağa bağlanmamalı ve bu cihazlardan herhangi bir veri alışverişi yapılmamalıdır(Örneğin taşınabilir disk takılmamalıdır).
- Bilgisayarlara takılan taşınabilir cihazlar her seferinde antivirüs yazılımı tarafından taranmalıdır.
- Gerekmedikçe klasörleri, dosyaları veya diskleri paylaşıma açma, okuma/yazma yetkileri verilmemelidir. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.
- Bilinmeyen veya şüpheli kaynaklardan asla dosya indirilmemelidir.
- Zararlı yazılımların kuruma ait ve/veya kurum tarafından yönetilen cihazlar ve altyapı bileşenleri üzerinde çalışmasını, kaydedilmesini ve aktarılmasını engellemek için oluşturulan "**Beyaz Liste**de" bulunan uygulamalar haricinde hiçbir uygulama(ücretli, ücretsiz, lisanslı, lisanssız vb. farketmeksizin) kurulmamalıdır. Beyaz Liste bilgi güvenliği gereği sadece KTÜN erişim websitesine login olduktan sonra erişilebilecek şekilde yayımlanır.
- **Beyaz Liste**ye eklenmesi talep edilen yazılımlar detayları(Yazılım Adı, Kullanım amacı, linki vb.) ile birlikte some@ktun.edu.tr adresine gönderilmelidir. SOME tarafından güvenlik açısından düşük riskli görülen yazılımlar listeye eklenir.
- Kuruma ait tüm cihazlarda kurumun lisanslı antivirüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.

- Hiçbir kullanıcı herhangi bir sebepten dolayı kuruma ait bir cihazdan antivirüs programını kaldıramaz ve başka bir antivirüs yazılımını cihaza kuramaz.
- Antivirüs yazılımı yüklü olmayan cihaz ağa bağlanmamalı ve hemen Bilgi İşlem Birimine haber verilmelidir.
- Etki alanına(Active Directory) dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartabilecektir.
- Virüs bulaşma ihtimaline karşı kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.
- Cihazlardaki dosyalar bilinen kişilerden gelse dahi mutlaka antivirüs taramasından geçirilmelidir.

6. Yaptırım

Bu politikanın ihlal edilmesi durumunda KTÜN BİLGİ GÜVENLİĞİ POLİTİKASI'nda belirtilen "POLİTİKANIN İHLALİ VE YAPTIRIMLAR" başlığı altındakiler geçerlidir.

7. 7. Yürürlük

Bu politika, BGYS komisyonu tarafından onaylandıktan sonra Bilgi İşlem Daire Başkanlığının web sayfasında yayımlanarak duyurusu yapıldığı tarihte yürürlüğe girer.

8. 8. Yürütme

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.