**ANTİVİRÜS KULLANIM PROSEDÜRÜ**

**GALLİNA EURASİA POLİKARBONAT SİSTEMLERİ SAN. VE TİC. LTD. ŞTİ.**

**1. Amaç**

Bu prosedürün amacı Gallina Eurasia Polikarbonat Sistemleri San. ve Tic. Ltd. Şti. bünyesinde kullanılan bilgisayarlar ve kötücül yazılımların tehdidinde olan tüm sistemlere yönelik anti-virüs kullanım esaslarının tanımlanmasıdır.

**2. Kapsam**

Şirket bünyesinde kullanılan tüm bilgisayarlar, kötücül yazılımların tehdidinde olan tüm sistemler ve bunları kullanan personel bu politika kapsamındadır.

**3. Sorumlular**

Bu politikanın oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Uygulanmasından sorumluluğundan herhangi bir bilgisayar veya kötücül yazılımların tehdidinde olan sistemleri kullanan personeller sorumludur.

**4. Uygulama**

**Tanımlama:** Politika maddeleri anlatılırken bilgisayarlar ve kötücül yazılımların tehdidinde olan tüm sistemler için genel olarak “bilgisayar” ifadesi kullanılacaktır.

* Kurumumuzun veya hizmet verdiğimiz kullanıcıların bütün bilgisayarlar, sunucular vs. sistemlerinde anti-virüs yazılımı yüklü olmalıdır.
* Anti-virüs yazılımları gerçek zamanlı (real time) koruma sağlayacak şekilde konfigüre edilmelidir.
* Anti- virüs yazılımı ve virüs tanımları otomatik olarak güncellenmelidir.
* Anti-virüs yazılımı yüklü olmayan bilgisayarlar ağa bağlanmamalıdır.
* Anti-virüs yazılımının devre dışı bırakıldığı zamanlarda başka önlemler alınmalıdır. Anti-virüs yazılımlarının veri tabanları güncellemeleri otomatik olarak yapılmalıdır. Virüs bulaşan makineler yayılma durumuna karşı kesinlikle kurum ortak ağından çıkarılmalı tam olarak temizleninceye kadar ağa bağlanmamalıdır. Bilgisayarlar belirlenmiş periyotlarla 6 ayı geçmeyecek sürelerde cihaz kullanım sorumlusu olan kişi tarafından anti-virüs yazılımı ile taranmalıdır. Bilgisayarlara takılan taşınabilir aygıtlar her takılmada anti-virüs yazılımı tarafından taranmalıdır. E-posta sunucusu mail yoluyla virüs ve benzeri tehditlerin sisteme dâhil olması durumu için kritik noktada olduğundan fazladan koruma içermelidir. Bilinmeyen veya şüpheli web sitelerinden asla dosya indirilmemelidir.
* Gerekmedikçe klasörleri, dosyaları veya diskleri paylaşıma açma, okuma/yazma yetkileri verilmemelidir.

**5. Yaptırım**

Bu prosedürün ihlal edilmesi durumunda yönetim tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel yönetim tarafından yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3’ten fazla tekrar ederse ilgili disiplin yaptırımları gereğince personel hakkında işlem yapılır.

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu prosedürün ihlallerini, en kısa sürede yönetime bildirme sorumluluğundadır.