1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında kullanılan bilgi varlıklarının virüs, solucan, truva atı, casus yazılım, fidye yazılımı ve diğer kötü amaçlı yazılımlara karşı korunmasına yönelik temel kuralları belirlemek ve kötü amaçlı yazılım kaynaklı bilgi güvenliği olaylarının önlenmesini sağlamaktır.

2. KAPSAM

Bu politika;

- Süleyman Demirel Üniversitesi Daire Başkanlıklarını,
- Genel Sekreterliği,
- Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimini,
- Kurum tarafından temin edilen veya kurum bilgi sistemlerine erişim sağlayan bilgisayar, sunucu ve diğer uç cihazları,
- Bu cihazlarda kullanılan işletim sistemi, uygulama ve güvenlik yazılımlarını kapsar

3. SORUMLULUKLAR

3.1. Bilgi İşlem Daire Başkanlığı

- Kötü amaçlı yazılımlara karşı koruma altyapısının kurulması, işletilmesi ve izlenmesinden,
- Antivirüs/anti-malware yazılımlarının güncel tutulmasından,
- Güvenlik yazılımlarının güncelleme ve imza/veri tabanı güncellemelerinin yönetilmesinden,
- Tespit edilen kötü amaçlı yazılımlara ilişkin gerekli teknik müdahalelerin gerçekleştirilmesinden,
- Bilgi güvenliği olaylarının ilgili süreçler kapsamında değerlendirilmesinden sorumludur.

3.2. Kullanıcılar

- Kurum tarafından sağlanan güvenlik yazılımlarını devre dışı bırakmamak,
- Antivirüs/anti-malware uyarılarını dikkate almak,
- Şüpheli e-posta, bağlantı, dosya ve yazılımları açmamak veya çalıştırmamak,
- Güvenilmeyen kaynaklardan dosya veya yazılım indirmemek,
- Kötü amaçlı yazılım şüphesi veya güvenlik olayı tespit ettiklerinde Bilgi İşlem Daire Başkanlığına bildirimde bulunmak ile yükümlüdür.

4. UYGULAMA

4.1. Güvenlik Yazılımlarının Kullanılması

Kurum tarafından yönetilen ve kötü amaçlı yazılım korumasına ihtiyaç duyulan bilgi sistemlerinde uygun antivirüs/anti-malware çözümleri kullanılmalıdır.

Güvenlik yazılımlarının;

- Gerçek zamanlı koruma özellikleri,
- Kötü amaçlı yazılım tespit ve engelleme mekanizmaları,
- Güncel imza/veri tabanı veya eşdeğer tehdit istihbaratı,
- Merkezi yönetim ve raporlama imkanları kurumun bilgi güvenliği ihtiyaçları doğrultusunda kullanılmalıdır.

4.2. Güncellemelerin Yönetilmesi

Antivirüs/anti-malware yazılımlarının güvenlik güncellemeleri ve imza/veri tabanı güncellemeleri mümkün olduğunca otomatik ve merkezi olarak gerçekleştirilmelidir. Güncellemelerin başarısız olması veya güvenlik yazılımının güncel olmaması durumunda gerekli teknik kontroller gerçekleştirilmelidir.

4.3. E-posta ve Dosya Güvenliği

Kullanıcılar;

- Kaynağı bilinmeyen veya şüpheli e-posta eklerini açmamalı,
- Şüpheli bağlantılara tıklamamalı,
- Şüpheli dosyaları çalıştırmamalı,
- Kimlik bilgisi veya hassas bilgi talep eden şüpheli e-postalara karşı dikkatli olmalı,
- Güvenilirliği doğrulanmamış kaynaklardan dosya veya yazılım indirmemelidir.

Şüpheli e-posta ve ekleri kurumun belirlediği bilgi güvenliği olay bildirim kanallarından Bilgi İşlem Daire Başkanlığına bildirilmelidir.

4.4. Kötü Amaçlı Yazılım Tespiti

Bir cihazda kötü amaçlı yazılım tespit edilmesi veya kötü amaçlı yazılım bulaştığından şüphelenilmesi halinde;

1. Cihazın ağ bağlantısı, olayın yayılmasını önlemek amacıyla gerekli görülmesi halinde kesilir veya sınırlandırılır.
2. Kullanıcı tarafından güvenlik yazılımı devre dışı bırakılmaz ve tespit edilen dosyalar üzerinde bilinçsiz müdahalede bulunulmaz.
3. Bilgi İşlem Daire Başkanlığına bildirim yapılır.
4. Gerekli teknik inceleme ve temizleme işlemleri gerçekleştirilir.
5. Olayın bilgi güvenliği olayı niteliğinde olması halinde ilgili olay yönetimi süreci işletilir.

6. Cihazın güvenli olduğunun değerlendirilmesinden sonra yeniden kurumsal ağa dahil edilmesi sağlanır.

4.5. Kötü Amaçlı Yazılım Üretimi ve Dağıtımı

Kurum bilgi sistemleri kullanılarak virüs, solucan, truva atı, fidye yazılımı veya diğer kötü amaçlı yazılımların oluşturulması, dağıtılması, çalıştırılması veya yayılmasına yönelik faaliyetlerde bulunulması yasaktır.

Güvenlik testleri ve yetkili teknik çalışmalar bu hükmün dışındadır. Bu tür çalışmalar yalnızca yetkilendirilmiş personel tarafından, belirlenmiş test ortamlarında ve ilgili prosedürlere uygun olarak gerçekleştirilir.

4.6. Spam ve Şüpheli Mesajlar

Spam, zincir mesajlar, şüpheli veya kötü amaçlı içerik barındırdığı değerlendirilen e-postalar açılmadan silinmeli ve gerekli görülmesi halinde Bilgi İşlem Daire Başkanlığına bildirilmelidir.

4.7. Güvenlik Yazılımının Devre Dışı Bırakılması

Kurum tarafından sağlanan antivirüs, anti-malware veya diğer uç nokta güvenlik kontrolleri kullanıcılar tarafından devre dışı bırakılamaz, kaldırılamaz veya güvenlik seviyesini azaltacak şekilde değiştirilemez.

Teknik zorunluluk nedeniyle yapılacak değişiklikler yalnızca yetkili Bilgi İşlem Daire Başkanlığı personeli tarafından gerçekleştirilir.

5. YAPTIRIM

Bu politikada belirtilen kurallara aykırı kullanım veya güvenlik kontrollerinin kasıtlı olarak devre dışı bırakılması durumunda, ilgili EYS süreçleri ve yürürlükteki mevzuat doğrultusunda gerekli işlemler uygulanır.