1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi bilişim sistemleri, bilgi varlıkları, ağ altyapısı ve elektronik iletişim ortamlarının siber saldırılar, kötü amaçlı yazılımlar, yetkisiz erişim, oltalama (phishing), zararlı bağlantı ve dosyalar ile diğer siber tehditlere karşı korunmasına yönelik temel güvenlik kurallarını ve uygulanacak önlemleri belirlemektir.

Bu kapsamda; siber saldırıların önlenmesi, tespit edilmesi, izlenmesi, saldırıların etkilerinin azaltılması ve meydana gelen güvenlik olaylarına uygun şekilde müdahale edilmesi amaçlanmaktadır.

2. KAPSAM

Bu politika; Süleyman Demirel Üniversitesi bünyesinde kullanılan sunucu, masaüstü ve dizüstü bilgisayarlar, mobil cihazlar, sanal sistemler, ağ ve iletişim altyapısı, elektronik posta sistemleri, internet erişim altyapısı, taşınabilir ve çıkarılabilir medya ortamları ile diğer bilişim sistemlerini kapsar.

Politika; Üniversitenin bilişim kaynaklarını kullanan tüm çalışanları, kullanıcıları, hizmet sağlayıcıları ve ilgili üçüncü tarafları kapsar.

3. SORUMLULUK

Bu politikanın uygulanmasından;

- **Bilgi İşlem Daire Başkanlığı**, siber saldırılara karşı gerekli teknik ve idari güvenlik önlemlerinin alınması, güvenlik altyapısının yönetilmesi, izlenmesi ve gerekli durumlarda müdahale edilmesinden,
- **Sistem yöneticileri**, sunucu, ağ ve diğer bilişim sistemlerinde güvenlik kontrollerinin uygulanması, güncellemelerin gerçekleştirilmesi, güvenlik kayıtlarının izlenmesi ve tespit edilen güvenlik olaylarının değerlendirilmesinden,
- **Tüm çalışanlar ve kullanıcılar**, bu politikaya uygun hareket etmekten, bilgi güvenliği kurallarına uymaktan ve şüpheli durumları gecikmeksizin Bilgi İşlem Daire Başkanlığına bildirmekten,
- **Hizmet sağlayıcılar ve ilgili üçüncü taraflar**, Üniversite bilişim sistemlerine erişimleri kapsamında belirlenen bilgi güvenliği kurallarına uymaktan sorumludur.

4. UYGULAMA

4.1. Siber Saldırılara Karşı Koruma

- Üniversitenin bilişim sistemleri siber saldırılara karşı risk değerlendirmesi sonuçları doğrultusunda uygun teknik ve idari güvenlik kontrolleri ile korunacaktır.
- Güvenlik duvarı, ağ güvenlik sistemleri, uç nokta güvenlik çözümleri, e-posta güvenlik sistemleri ve benzeri güvenlik mekanizmaları yetkisiz erişim ve kötü amaçlı faaliyetlerin önlenmesi amacıyla kullanılacaktır.
- Siber saldırıların tespit edilmesi veya saldırı şüphesi oluşması halinde gerekli güvenlik önlemleri alınacak ve ilgili sistemler gerektiğinde izole edilecek veya erişimleri sınırlandırılacaktır.

4.2. Kötü Amaçlı Yazılımlardan Korunma

- Üniversite bilişim sistemlerinde kullanılan uygun uç cihazlar ve sunucular, Bilgi İşlem Daire Başkanlığı tarafından onaylanan güncel kötü amaçlı yazılımlardan korunma çözümleri ile korunacaktır.
- Antivirüs ve benzeri güvenlik yazılımlarının gerçek zamanlı koruma, tarama, tespit ve karantina özellikleri mümkün olduğunca etkin tutulacaktır.
- Kötü amaçlı yazılımlardan korunma sistemlerinin imza, motor ve güvenlik bileşenleri merkezi olarak ve mümkün olduğunca otomatik şekilde güncellenecektir.
- Kötü amaçlı yazılım tespit edilmesi halinde ilgili dosya, sistem veya cihaz için gerekli karantina, izolasyon, temizleme veya yeniden kurulum işlemleri uygulanacaktır.
- Kötü amaçlı yazılım koruma sistemleri tarafından oluşturulan kritik uyarılar takip edilecek ve gerekli durumlarda olay yönetim süreci başlatılacaktır.

4.3. E-Posta ve Oltalama Saldırılarına Karşı Koruma

- Bilinmeyen veya güvenilmeyen kaynaklardan gelen e-posta, mesaj, bağlantı ve dosya ekleri dikkatle değerlendirilecek ve şüpheli içerikler açılmayacaktır.
- E-posta ve e-posta ekleri, Üniversitenin kullandığı güvenlik altyapısının izin verdiği ölçüde kötü amaçlı yazılım, spam ve zararlı içerik açısından taranacaktır.
- Kullanıcılar kendilerinden parola, kullanıcı adı, doğrulama kodu veya gizli bilgi isteyen şüpheli e-posta ve mesajlara cevap vermeyecektir.
- Oltalama (phishing) veya sosyal mühendislik saldırısı şüphesi bulunan e-posta, mesaj veya bağlantılar Bilgi İşlem Daire Başkanlığına ivedilikle bildirilecektir.

4.4. Taşınabilir ve Çıkarılabilir Medya Güvenliği

- USB bellek, harici disk, CD/DVD ve benzeri çıkarılabilir medya ortamları Üniversite bilişim sistemlerinde kullanılmadan önce gerekli güvenlik kontrollerinden geçirilecektir.

- Güvenilir olmayan kaynaklardan temin edilen veya kaynağı bilinmeyen taşınabilir medya ortamlarının kullanılması sınırlandırılabilir veya engellenebilir.
- Taşınabilir medya yoluyla kötü amaçlı yazılım bulaşmasının önlenmesi amacıyla gerekli teknik kontroller uygulanacaktır.

4.5. Güvenlik Güncellemeleri ve Teknik Zafiyetler

- İşletim sistemi, uygulama, sunucu, ağ cihazı ve güvenlik bileşenlerine ilişkin güvenlik güncellemeleri ve yamalar, belirlenen yama ve güncelleme süreçlerine uygun olarak uygulanacaktır.
- Kritik güvenlik zafiyetleri risk seviyeleri dikkate alınarak öncelikli olarak değerlendirilecek ve gerekli teknik önlemler alınacaktır.
- Güncel olmayan veya güvenlik açısından risk oluşturan yazılım ve bileşenlerin kullanımı gerekli durumlarda sınırlandırılacak veya sonlandırılacaktır.

4.6. Ağ Güvenliği ve Uzaktan Erişim

- Üniversite bilişim ağına dışarıdan bağlanması gerekli olan yetkili kullanıcılar, Bilgi İşlem Daire Başkanlığı tarafından belirlenen güvenli uzaktan erişim yöntemlerini kullanacaktır.
- Uzaktan erişimlerde VPN veya Üniversite tarafından onaylanan diğer güvenli erişim yöntemleri kullanılacaktır.
- Güvenlik duvarı ve diğer ağ güvenlik sistemleri aracılığıyla yetkisiz veya şüpheli bağlantılar gerekli durumlarda engellenecektir.
- Ağ güvenlik kuralları ve erişim yetkileri, bilgi güvenliği riskleri ve iş ihtiyaçları doğrultusunda düzenli olarak gözden geçirilecektir.

4.7. Güvenlik Kayıtları ve İzleme

- Güvenlik duvarı, antivirüs, sunucu, ağ cihazları, e-posta güvenlik sistemleri ve diğer uygun sistemler tarafından oluşturulan güvenlik kayıtları, belirlenen süreçler kapsamında tutulacak ve gerektiğinde incelenecektir.
- Kritik güvenlik olaylarına ilişkin alarm ve kayıtlar Bilgi İşlem Daire Başkanlığı tarafından izlenecek ve değerlendirilecektir.
- Güvenlik kayıtlarının yetkisiz şekilde değiştirilmesini, silinmesini veya erişilmesini önlemek amacıyla gerekli teknik ve idari tedbirler uygulanacaktır.

4.8. Kullanıcı Güvenliği

- Üniversite personeli; e-posta, telefon, mesajlaşma uygulamaları veya diğer iletişim kanalları aracılığıyla kendisinden istenen parola, kullanıcı adı, doğrulama kodu veya diğer gizli kimlik doğrulama bilgilerini üçüncü kişilerle paylaşmayacaktır.
- Kullanıcılar, kendilerine tahsis edilen bilişim kaynaklarını güvenlik politikalarına uygun şekilde kullanacaktır.
- Bilgi İşlem Daire Başkanlığı tarafından kurulmuş veya yönetilen antivirüs, spam koruma, güvenlik duvarı ve benzeri güvenlik mekanizmaları kullanıcılar tarafından devre dışı bırakılamaz, kaldırılamaz veya yetkisiz şekilde değiştirilemez.
- Bilgi İşlem Daire Başkanlığı Sistem Yöneticileri tarafından güvenlik gerekçesiyle kullanılması yasaklanan veya kısıtlanan yazılım ve bileşenler Üniversite bilişim sistemlerinde kullanılmayacaktır.

4.9. Siber Olayların Bildirilmesi ve Müdahale

- Siber saldırı, kötü amaçlı yazılım, yetkisiz erişim, oltalama veya diğer bilgi güvenliği olaylarının tespit edilmesi ya da şüphelenilmesi halinde durum gecikmeksizin Bilgi İşlem Daire Başkanlığına bildirilecektir.
- Siber olayların değerlendirilmesi ve müdahalesi, Üniversitenin bilgi güvenliği olay yönetimi süreçlerine uygun olarak gerçekleştirilecektir.
- Gerekli durumlarda saldırıya maruz kalan sistem ağdan izole edilecek, ilgili hesap veya erişimler geçici olarak kısıtlanacak ve saldırının yayılmasını önleyici tedbirler alınacaktır.
- Olay sırasında oluşan sistem, ağ, güvenlik ve diğer ilgili kayıtlar, olayın incelenmesi ve gerekli durumlarda kanıt niteliğinin korunması amacıyla muhafaza edilecektir.

4.10. Olay Sonrası Değerlendirme ve İyileştirme

- Gerçekleşen siber güvenlik olayları sonrasında olayın nedeni, etkileri, alınan önlemler ve tekrarını önlemeye yönelik yapılabilecek iyileştirmeler değerlendirilecektir.
- Gerekli görülen durumlarda düzeltici faaliyet, risk değerlendirmesi, teknik iyileştirme veya ilave güvenlik kontrolü gerçekleştirilecektir.
- Önemli siber güvenlik olaylarından elde edilen deneyimler, bilgi güvenliği süreçlerinin ve kontrollerinin geliştirilmesinde kullanılacaktır.

4.11. Farkındalık

- Çalışanlara siber saldırılar, kötü amaçlı yazılımlar, oltalama saldırıları, sosyal mühendislik, şüpheli e-posta ve bağlantılar ile bilgi güvenliği olaylarının bildirilmesi konularında farkındalık faaliyetleri gerçekleştirilecektir.
- Gerektiğinde oltalama simülasyonları, bilgilendirme duyuruları veya diğer farkındalık çalışmaları uygulanabilecektir.

5. YAPTIRIM

Bu politikaya aykırı hareket edildiğinin tespit edilmesi halinde ilgili durum, Üniversitenin bilgi güvenliği olay yönetimi, uygunsuzluk ve düzeltici faaliyet süreçlerine göre değerlendirilecektir.

Gerekli görülmesi halinde teknik, idari ve düzeltici faaliyetler uygulanacaktır.