1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında bilgi varlıklarının gizliliğinin, bütünlüğünün, kimlik doğrulamasının ve gerektiğinde inkâr edilemezliğinin sağlanması amacıyla kullanılan kriptografik kontrollerin güvenli ve etkin şekilde yönetilmesine ilişkin esasları belirlemektir.

Bu politika ile;

- bilgilerin yetkisiz kişilerce okunmasının önlenmesi,
- bilgi bütünlüğünün korunması,
- kimlik doğrulama ve güvenli iletişimin desteklenmesi,
- elektronik imza ve sertifika hizmetlerinin güvenli şekilde kullanılması,
- kriptografik anahtarların yaşam döngüsünün güvenli şekilde yönetilmesi,
- güncelliğini yitirmiş veya güvenli kabul edilmeyen algoritma ve protokollerin kullanımının önlenmesi amaçlanmaktadır.

2. KAPSAM

Bu politika; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi bünyesinde kullanılan ve kriptografik kontrol gerektiren;

- bilgi sistemlerini,
- sunucu ve ağ altyapısını,
- uygulamaları,
- veri tabanlarını,
- iletişim kanallarını,
- elektronik imza ve sertifika hizmetlerini,
- VPN ve uzaktan erişim çözümlerini,
- şifreleme anahtarlarını,
- kriptografik donanım ve yazılımları kapsar.

Politika ayrıca bu sistemleri yöneten BİDB personeli, ilgili birim personeli, hizmet sağlayıcılar ve kriptografik kontrollere erişimi bulunan diğer yetkili kişileri kapsar.

3. SORUMLULUKLAR

3.1. Bilgi İşlem Daire Başkanlığı

- Üniversitenin bilgi sistemlerinde kullanılan kriptografik kontrollerin koordinasyonundan,
- onaylı algoritma ve protokollerin belirlenmesi ve uygulanmasından,
- kriptografik anahtarların güvenli yönetiminin sağlanmasından,
- sertifika ve sertifika yaşam döngüsünün yönetilmesinden,
- kriptografik kontrollerin teknik olarak izlenmesinden,

- güvenliğini kaybetmiş algoritma ve protokollerin değiştirilmesinin planlanmasından sorumludur.

3.2. Sistem ve Ağ Birimi

- Sunucu, ağ, VPN, TLS ve benzeri altyapılarda kullanılan kriptografik yapılandırmaların yönetilmesinden,
- Sertifikaların kurulumu, yenilenmesi ve gerektiğinde iptal edilmesinden,
- Kriptografik anahtarların güvenli şekilde saklanmasından,
- Güvenlik zafiyeti bulunan protokol ve algoritmaların tespit edilmesi ve değiştirilmesinden sorumludur.

3.3. Yazılım ve Web Geliştirme Birimi

- Geliştirdiği uygulamalarda onaylı kriptografik yöntemlerin kullanılmasından,
- Hassas bilgilerin uygun yöntemlerle korunmasından,
- Parola ve kimlik doğrulama bilgilerinin güvenli şekilde saklanmasından,
- Uygulamalarda güvenli kriptografik kütüphane ve mekanizmaların kullanılmasından sorumludur.

3.4. Sistem ve Bilgi Varlığı Sorumluları

Sistem ve bilgi varlığı sorumluları, kendi sorumluluklarındaki sistemlerde kullanılan kriptografik kontrollerin bu politika ve ilgili teknik standartlara uygun olmasını sağlar.

4. UYGULAMA

4.1. Kriptografik Kontrollerin Kullanımı

- Kriptografik kontroller;
  - Bilgilerin gizliliğini sağlamak,
  - Bütünlüğünü korumak,
  - Gönderici ve alıcının kimliklerini doğrulamak,
  - Güvenli iletişimin sağlanması,
  - Elektronik imsa uygulamalarının gerçekleştirilmesi,
  - bilgi veya işlemin kaynağının doğrulanmasının desteklenmesi amacıyla kullanılır.

- Kriptografik yöntem seçilirken;
  - bilginin sınıflandırma seviyesi,
  - bilgi güvenliği riski,
  - kişisel verilerin niteliği,
  - sistemin kritiklik seviyesi,
  - uygulamanın güvenlik gereksinimleri,
  - yasal ve düzenleyici yükümlülükler,
  - kullanılan teknolojinin güncelliği,

- algoritmanın güvenlik seviyesi,
- anahtar uzunluğu,
- birlikte çalışabilirlik gereksinimleri dikkate alınır.

- Kriptografik kontroller, yalnızca onaylanmış amaçlar ve kullanım senaryoları için kullanılır.

4.2. Onaylı Kriptografik Algoritmalar

Üniversite bilgi sistemlerinde kullanılacak algoritmalar, güncel güvenlik gereksinimleri ve ilgili teknik standartlar dikkate alınarak belirlenir.

Kriptografik yöntem	**Asgari tercih**	**Kullanım amacı**
AES	AES-256 veya güncel güvenlik gereksinimini karşılayan eşdeğer	Durağan verilerin ve iletişim kanallarının şifrelenmesi
RSA	RSA-2048 ve üzeri; yeni sistemlerde risk ve teknoloji gereksinimine göre daha güçlü anahtarlar	Elektronik imza, sertifika ve anahtar değişimi
ECC	Kurumca onaylanan güncel eğri ve anahtar uzunluğu	Elektronik imza, anahtar değişimi ve kimlik doğrulama
SHA-2 / SHA-3	SHA-256 ve üzeri	Veri bütünlüğü, dijital imza ve güvenli özetleme

SHA-2 ve SHA-3 ailesi **şifreleme amacıyla değil**, veri bütünlüğü, özetleme ve uygun kullanım senaryolarında parola türetme veya doğrulama mekanizmalarının bir parçası olarak kullanılır.

Parolalar düz metin olarak saklanamaz.

4.3. Kullanılması Yasaklanan Veya Kaçınılması Gereken Yöntemler

Aşağıdaki algoritma ve protokoller yeni sistemlerde kullanılmaz:

Yöntem	**Durum**	**Tercih Edilecek Yaklaşım**
DES	Yasak	AES veya güncel güvenli simetrik algoritma
3DES	Yeni sistemlerde kullanılmaz	AES veya güncel güvenli algoritma

SHA-1	Güvenlik amacıyla kullanılmaz	SHA-2 / SHA-3
RC4	Yasak	AES veya güncel güvenli algoritma
SSLv2	Yasak	TLS
SSLv3	Yasak	TLS
TLS 1.0	Yasak	Güncel TLS sürümü
TLS 1.1	Yasak	Güncel TLS sürümü
SSHv1	Yasak	SSHv2
PPTP	Kullanılmaz	IPsec VPN veya TLS tabanlı güvenli VPN

Mevcut sistemlerde güvenliği zayıflamış algoritma veya protokollerin bulunması halinde risk değerlendirmesi yapılır ve uygun bir geçiş planı oluşturulur.

Güvenlik seviyesi yetersiz hale gelen algoritma ve protokoller yeni sistemlerde uygulanamaz.

4.4. Kriptografik Protokoller

4.4.1. TLS

1. Güvenli web erişimi ve uygun diğer iletişim senaryolarında TLS kullanılır.
2. Yeni sistemlerde güvenli ve güncel TLS yapılandırmaları kullanılır.
3. Güvenliği zayıflamış TLS sürümleri ve şifre takımları devre dışı bırakılır.
4. TLS yapılandırmalarında kullanılan sertifikaların geçerlilik süresi, güvenilir sertifika otoritesi, anahtar uzunluğu ve kriptografik özellikleri kontrol edilir.

4.4.2. SSH

Uzaktan yönetim ve güvenli dosya aktarımı gibi ihtiyaçlarda SSHv2 kullanılır.

4.4.3. IPsec / VPN

Güvenli uzaktan erişim veya site-to-site bağlantılarda kurum tarafından onaylanan IPsec veya TLS tabanlı VPN çözümleri kullanılır.

4.4.4. S/MIME

Elektronik posta içeriğinin gizliliği ve bütünlüğünün korunması veya elektronik imza gereksinimlerinde kurum tarafından uygun görülmesi halinde S/MIME gibi güvenli mekanizmalar kullanılabilir.

4.5. Sertifika Yönetimi

1. Kurumsal sistemlerde kullanılan dijital sertifikalar yetkili sertifika otoritelerinden veya Üniversite tarafından yetkilendirilmiş iç sertifika altyapısından temin edilir.
2. Sertifikaların;

    - geçerlilik süresi,
    - sertifika otoritesi,
    - kullanım amacı,
    - alan adı,
    - anahtar uzunluğu,
    - kriptografik algoritması,
    - iptal durumu izlenir.

3. Sertifikaların süresi dolmadan önce yenilenmesi sağlanır.
4. Güvenliği ihlal edilen, hatalı oluşturulan veya artık kullanılmayan sertifikalar gerektiğinde iptal edilir.
5. İnternete açık sistemlerde kullanılan sertifikaların güvenilir sertifika otoritelerinden temin edilmesi esastır.
6. İç sistemlerde, kurumun güvenlik gereksinimleri doğrultusunda kurum içi CA kullanılabilir.
7. Geliştirme ve test ortamlarında self-signed sertifikalar yalnızca izole ve kontrollü ortamlarda kullanılabilir. Canlı ve internete açık sistemlerde kullanılmaz.
8. Wildcard sertifikaların kullanımı güvenlik riski ve sistem mimarisi dikkate alınarak değerlendirilir. Kritik sistemlerde mümkün olduğunda sistem veya hizmet bazlı ayrı sertifikalar tercih edilir.
9. Sertifikaların iptal durumlarının kontrolünde uygun mekanizmalar, teknik gereksinimlere göre CRL ve/veya OCSP gibi yöntemler kullanılabilir.

4.6. Elektronik İmza

1. Elektronik imza uygulamalarında ilgili mevzuat ve kurum tarafından onaylanan elektronik imza hizmetleri kullanılır.
2. Elektronik imza oluşturma ve doğrulama verileri yetkisiz kişilerden korunur.
3. Elektronik imza araçları, PIN ve benzeri kimlik doğrulama bilgileri başka kişilerle paylaşılmaz.
4. Elektronik imza sertifikalarının geçerlilik süresi ve gerektiğinde iptal/yenileme işlemleri takip edilir.
5. Elektronik imza hizmetlerinde meydana gelen arızalar veya erişim sorunlarında yetkili teknik destek ve ilgili hizmet sağlayıcılarla iletişim kurulur.

6. Elektronik imzanın kullanımı ve hukuki geçerliliği 5070 sayılı Elektronik İmza Kanunu ve ilgili mevzuat kapsamında değerlendirilir.

4.7. Kriptografik Anahtarların Yönetimi

Kriptografik anahtarlar yaşam döngüleri boyunca güvenli şekilde yönetilir. Anahtar yönetimi aşağıdaki süreçleri kapsar:

- anahtar oluşturma,
- anahtarın yetkilendirilmesi,
- güvenli dağıtımı,
- etkinleştirilmesi,
- güvenli şekilde saklanması,
- yedeklenmesi,
- gerektiğinde kurtarılması,
- yenilenmesi,
- değiştirilmesi,
- iptal edilmesi,
- kullanım dışı bırakılması,
- güvenli şekilde imha edilmesi.

4.8. Anahtarların Korunması

1. Kriptografik anahtarlar yalnızca yetkilendirilmiş kişiler ve sistemler tarafından kullanılabilir.
2. Kritik anahtarlar mümkün olduğunda güvenli anahtar kasalarında, donanımsal güvenlik modüllerinde (HSM) veya güvenli anahtar yönetim sistemlerinde saklanır.
3. Anahtarlar düz metin olarak yetkisiz ortamlarda saklanamaz.
4. Anahtarların erişim yetkileri görev ve sorumluluklara göre sınırlandırılır.
5. Anahtarlara erişim ve anahtar üzerinde gerçekleştirilen kritik işlemler, sistemin teknik imkânları doğrultusunda kayıt altına alınır.

4.8.1. Anahtarların Yenilenmesi ve İptali

Aşağıdaki durumlarda anahtarların değiştirilmesi veya iptal edilmesi değerlendirilir:

- anahtarın ele geçirildiğinden şüphelenilmesi,
- anahtarın güvenliğinin ihlal edilmesi,
- anahtarın kullanım süresinin sona ermesi,
- algoritmanın güvenlik seviyesinin yetersiz hale gelmesi,
- sistem veya uygulama değişikliği,
- anahtar sahibinin görev veya yetkisinin değişmesi,
- ilgili sertifikanın iptal edilmesi.

4.8.2. Anahtarların Yedeklenmesi

Kritik sistemlerin sürekliliği için gerekli olan kriptografik anahtarlar, risk değerlendirmesi ve iş sürekliliği gereksinimleri doğrultusunda güvenli şekilde yedeklenebilir. Yedek anahtarlara erişim yalnızca yetkilendirilmiş kişilerle sınırlandırılır.

4.8.3. Anahtarların İmhası

Kullanım süresi sona eren, güvenliği ihlal edilen veya artık ihtiyaç duyulmayan kriptografik anahtarlar, ilgili bilgi ve sistem gereksinimleri dikkate alınarak güvenli yöntemlerle imha edilir. Arşivlenmiş bilgilerin erişilebilirliğinin korunması gereken durumlarda anahtar geçmişi ve gerekli metadata güvenli şekilde muhafaza edilir.

4.9. Kriptografik Kontrollerin Gözden Geçirilmesi

Kriptografik algoritmalar, protokoller ve anahtar yönetim yöntemleri;

- güvenlik tehditlerindeki değişiklikler,
- teknolojik gelişmeler,
- güvenlik zafiyetleri,
- yasal ve düzenleyici gereklilikler,
- risk değerlendirmeleri,
- üretici ve güvenilir güvenlik kaynaklarının duyuruları dikkate alınarak belirlenen periyotlarda gözden geçirilir.

Güvenliği yetersiz hale gelen kriptografik yöntemlerin değiştirilmesi için gerekli düzeltici veya iyileştirici faaliyetler başlatılır.

5. YAPTIRIM

Bu politikaya aykırı hareket eden çalışanlar ve diğer ilgili taraflar hakkında olayın niteliğine göre ilgili EYS süreçleri, sözleşme hükümleri, ilgili mevzuat ve Üniversitenin disiplin hükümleri uygulanır.