1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde kurumun gizliliği, aslına uygunluğu ve/veya bütünlüğünün korunması için Kriptografi'nin doğru ve etkin kullanımını temin etmektir.

2. KAPSAM

Bu politika, Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı 'nın tüm kriptografik kontrollerini kapsar.

3. SORUMLULUKLAR

Bu Politikanın uygulanmasından, Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı Yazılım ve Web Geliştirme Birimi ve Sistem ve Ağ Birimi sorumludur.

4. UYGULAMA

- Kriptografik kontroller;
    - Bilgilerin gizliliğini sağlamak,
    - Bütünlüğünü korumak,
    - Gönderici ve alıcının kimliklerini doğrulamak,
    - Yapılan işlemlerin hiçbir şekilde inkâr edilmemesini ve
    - Özgünlük ve güvenilirliği garanti etmek amacıyla kullanılır.

- Kriptografik yöntem uygulanırken, verinin geriye dönük elde edilememesi düşünülerek yedeklenir.
- Elektronik, yazılım ve donanımları, erişimi kontrol eden parolalar uygun ve güvenli bir konumda korunur,
- Elektronik imza sistem ve servislerinde problem olması durumunda erişim yapılacak kişilerin iletişim bilgileri, erişilebilir bir konumda olmalıdır.
- 2. ve 3. Taraf servislere SSL sertifikası girilmek istenmesi durumunda o servise özel SSL sertifikası üretilir. Wildcard sertifika vermek diğer servislerin güvenliğini düşürmektedir.

- Şifreleme, bilgilerin gizliliğini sağlamak amacıyla yapılır. Şifrelenmiş bir bilgi, kötü niyetli bir kişinin eline geçse dahi okunamayacağı, erişilemeyeceği için önemli bir koruma sağlar.
- Elektronik (sayısal) sertifikalar, imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır. Bu bağlamda sertifika, ilgili kişi veya cihazın elektronik ortamdaki kimlik kartlarına benzetilebilir. Bilgisayar ortamında yapılacak işlemler tarafların sayısal sertifikaları ile yapılıyor ise ilgili kişilerin kimlikleri kesin olarak doğrulanabilir.
- e-İmza, elektronik dokümanları (E-posta, Ms Excel dosyası, Ms Word dosyası gibi) imzalamak için kullanılan ve bu elektronik dokümanı alan kişinin de, gönderen kişinin kim olduğuna emin olmasını ve güvenmesini sağlayan bir elektronik koddur. Dijital imza diğer adıyla elektronik imza ülkemizde 23.01.2004 yılında Resmi Gazetede yayınlanmış ve 23.07.2004'te yürürlüğe girmiş 5070 sayılı Elektronik İmza Kanunu ile de tanımlanmıştır.
- Tüm bu kriptografik işlemler (simetrik/asimetrik şifreleme, e-İmza vb.) çeşitli yazılım ve bazen de donanımların kullanılması suretiyle yapılır. Yapılan kriptografik işlemin beklenen faydayı sağlaması için güçlü kriptolama algoritmaları seçmek ve seçilecek algoritmaya göre yeterli koruma sağlayacak uzunlukta anahtar kullanmak gerekir. Zayıf bir algoritma ve yeteri kadar uzun olmayan bir anahtar ile yapılan işlemler güçlü bilgisayarlar ile kolayca çözülebilir.
    - Şifreleme yöntemlerinin seçiminde aşağıdaki hususlar dikkate alınır:
        - Yasal Yükümlülükler
        - Kriptografik yöntemlerin kullanılmasıyla ilişkili riskler
        - Kriptografik yöntemin güvenlik seviyesi
        - Uygulamanın güvenlik gereksinimi
        - Lisans Koşulları
- Onaylı şifreleme yöntemleri ve anahtarları, yalnızca onaylandıkları amaçlar için kullanılır.
- Kurum bilgisinin korunmasında kullanılmak üzere onaylanmış algoritmalar aşağıda belirtilmiştir.

Algoritma	Anahtar Boyutu	Kullanım Alanları
AES	256 bit ya da üstü	• Durağan veri şifrelemesi • Veri İletimi Şifrelemesi • TLS oturum anahtarı • Dijital İmza
RSA	2048 bit ya da üstü	• Anahtar değişimi • Simetrik anahtar şifreleme • Elektronik İmza • SSH • S/MI)ME • IPsec VPN • SSL VPN • Yazılım projeleri
SHA-2 SHA-3	256 bit ya da üstü	• Veri bütünlüğü • Parola saklama
DES -3DES	56 bit	• Yazılım Projeleri

- Kurum bilgisinin korunmasında kullanılmak üzere, uygulama gereksinimlerine ve yalnızca onaylı şifreleme algoritmalarını uygulamak üzere yapılandırıldığı durumda onaylanmış protokoller aşağıda belirtilmiştir.

Algoritma	Anahtar Boyutu	Kullanım Alanları
SSH	v2 ya da daha üstü	• Güvenli uzaktan erişim • Güvenli dosya aktarımı (SFTP) • Güvenli GUI-X11 • Güvenli dosya kopyalama (SCP)
TLS	v1.2 ya da daha üstü	• Güvenli web erişimi (HTTPS)

		• Güvenli veri aktarımı • Uçtan uca (Site to Site) VPN • Güvenli dizin erişimi (LDAPS) • IP üzerinden güvenli ses – SIP • Kimlik Doğrulama (Authentication)
S/MIME	V3 ya da daha üstü	• E-Posta gizliliği ve bütünlüğü için tünelleme
IPSEC		• Güvenli veri aktarımı • Uçtan uca (Site to Site) VPN

- Şifreleme algoritmalarının kullanımdan kalkması durumundan, onaylanmış ve yasaklanmış şifreleme yöntemleri en kısa zamanda gözden geçirilir.
- Kullanımdan kalkan şifreleme yöntemleri (algoritmalar ve protokoller), herhangi bir yeni sistemde uygulanamaz. Söz konusu yöntemler, İnternet'e erişen sistemlerde altı ay içerisinde onaylanmış yöntemlerle değiştirilebilir. İnternete erişmeyen iç sistemlerde, bilginin gizlilik ve bütünlük riskleriyle orantılı etki değerlendirilmesi sonrasında karar verilir.
- Bazı kullanımdan kalkan yöntemlerin, güncel web sunucularında, tarayıcılarda, cihazlarda, uygulamalarda ve işletim sistemlerinde hala varsayılan olarak etkin olabilmesi nedeniyle, tüm varsayılan ayarların kurulumdan sonra değiştirilmesine dikkat edilir.

- Aşağıdaki şifreleme yöntemlerinin kurum bünyesinde kullanılması yasaktır.

Yasaklanan Yöntem	**Önerilen Yöntem**
SHA-1	SHA-2 YA DA SHA -3
SSL v2 – SSL v3	TLS v1.2 ya da üstü
TLS v1.0	TLS v1.2 ya da üstü
SSH v1.x	SSH v2.x

PPTP	IPSEC ya da TLS
RC4- RC5	AES 256

- Kurum bünyesindeki uygulamalarda SSL /TLS sertifikaları ile ilgili olarak aşağıdaki tablodan yararlanılır.

Sef-Signed	
Onaylı Kullanım	İzole geliştirme ve test ortamları
Yasaklamış Kullanım	Canlı sistemler, internete açık sistemler
Geçerlilik süresi	-
Dahili CA	
Onaylı Kullanım	Dahili canlı sistemleri dahili Pre-Prod sistemler, dahili web sistemleri
Yasaklamış Kullanım	Canlı sistemler, internete açık sistemler
Geçerlilik süresi	-
DV	
Onaylı Kullanım	Kullanılmaz
Yasaklamış Kullanım	Kullanılmaz
Geçerlilik süresi	-
OV	
Onaylı Kullanım	İnternete yayın yapan, çok yoğun kullanılmayan ya da güçlü bir güvenlik düzeyi gerektirmeyen web sistemleri
Yasaklamış Kullanım	KVKK kapsamındaki verilerin işlendiği sistemler
Geçerlilik süresi	2 yıl
EV	
Onaylı Kullanım	İnternete yayın yapan, BGYS kapsamındaki paydaşlar tarafından kullanılması amaçlanan, yüksek düzeyde güvenlik gereksinimi bulunan, KVKK kapsamındaki verilerin işlendiği sistemler
Yasaklamış Kullanım	-
Geçerlilik süresi	2 yıl

- Üçüncü taraf sertifikalarının her biri, mümkünse, sunuculara ya da URL'lere tek tek uygulanmalıdır. Wildcard üçüncü taraf sertifikalar kullanılabilir.
- Her sertifika, CRL (Sertificate Revocation List) bilgilerini içermelidir.
- Halka açık web sistemleri, kullanıcı kimlik doğrulamayı geliştirmek amacıyla OCSP (Online Certificate Status Protocol) kullanılacak şekilde yapılandırılmalıdır.
- Halka açık web sitelerinde TLS üçüncü taraf içeriğini de içerecek şekilde kullanılmalıdır.

Şifreleme Anahtarlarının Yönetimi

- Şifreleme anahtarları, tahsis edilmiş anahtarları kullanıma ve koruma konusundaki sorumlulukları kendilerine bildirilmiş, bu konuda bilinçli kişilerin kullanımına verilir.
- Tüm şifreleme anahtarları, yaşam döngüleri boyunca yönetilmeli, izlenmeli ve kontrol edilmelidir.
- Mümkün olduğu durumlarda şifreleme anahtarları güvenli şifreleme kasalarıyla ya da güvenli uygulama şifreleme modüllerinde saklanmalıdır.
- Şifreleme anahtarlarının saklandığı alanlara her erişim girişimi, en az aşağıdaki bilgileri içerecek şekilde kaydedilmelidir.
    - Erişim girişiminin yapıldığı tarih ve saat
    - Erişim girişimi için kullanılan hesaplar
    - Kaynak sistem detayları (Hostname, IP adresi vb)
    - Girişimin başarılı olup olmadığı
    - Görüntülenen / erişilen /kopyalanan anahtarlar.
- Yeni şifreleme anahtarlarının oluşturulması kaydedilmeli ve uygulanabilirse, değişiklik yönetim süreci ile yönetilmelidir.
    - Bir şifreleme anahtarının yaşam döngüsü en az aşağıdaki aşamaları içerir:
    - Onaylı anahtar uzunlukları kullanılarak şifreleme anahtarlarının oluşturulması
    - Şifreleme anahtarlarının güvenli dağıtımı, etkinleştirilmesi ve saklanması, kurtarılması ve değiştirilmesi ya da güncellenmesi
    - Anahtarın güvenliğinin ihlal edildiğinde ya da anahtar sahibinin iş/görev değişikliğinde derhal iptal edilmesi
    - Kaybolmuş, bozulmuş ya da süresi dolmuş şifreleme anahtarlarının kurtarılması

- Şifreleme anahtarlarının yedeklenmesi ve arşivlenmiş bilgilere erişimi sağlayabilmek için anahtar geçmişinin korunması
- Hassas bilgilerin ve kritik sistemlerin korunması için gerekli şifreleme anahtarlarının paylaşılması.

5. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında **Disiplin Prosedürü** hükümleri uygulanır.

6. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	22.01.2020	İlk yayın.
001	7.11.2023	Uygulama kısmı detaylı olarak güncellenmiştir.