1. AMAÇ

Bu politikanın amacı bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunmasıdır.

2. KAPSAM

Bu politika, Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı 'nın tüm bilgi varlıklarını kapsar ve uygulanmasından bilgi varlıklarını kullanmakta olan tüm personel sorumludur.

3. SORUMLULUKLAR

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

4. UYGULAMA

Gizlilik: Bilgi, istenmeyen kişiler tarafından anlaşılmamalıdır.

Bütünlük: Bir iletinin alıcısı bu iletinin iletim sırasında değişikliğe uğrayıp uğramadığını öğrenmek isteyebilir; davetsiz bir misafir doğru iletinin yerine yanlış bir ileti koyma şansına erişmemelidir. Saklanan veya iletilmek istenen bilgi farkına varılmadan değiştirilememelidir.

Reddedilemezlik: Bilgiyi oluşturan ya da gönderen, daha sonra bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkar edememelidir. Bir gönderici daha sonrasında bir ileti göndermiş olduğunu yanlışlıkla reddetmemelidir.

Kimlik Belirleme: Gönderen ve alıcı, birbirlerinin kimliklerini doğrulayabilirler. Davetsiz bir misafir başkasının kimliğine bürünme şansına erişmemelidir.

Kriptografik Yöntemlere Güven: Kriptografik yöntemler, bilgi ve iletişim sistemlerinin kullanılması için güven oluşturmalıdır.

Özgür Seçim: Kullanılacak kriptografik ürünler, yasalar çerçevesinde özgürce seçilebilmelidir.

Gereksinime Bağlı Gelişme: Kriptografik yöntemler, birey, kurum ve hükümetlerin gereksinim, istem ve sorumluluklarına bağlı olarak gelişmelidirler.

Standartlar: Açık anahtar altyapısı ve şifreleme standartları ulusal ve uluslararası düzeylerde geliştirilmeli ve yaygınlaştırılmalıdır.

Bireysel Gizlilik Hakkı: Ulusal politikalar, bireysel iletişimin gizliliğine ve kişisel bilgilerin korunması gereğine saygı göstermelidir.

Yasal Erişim: Ulusal politikalar, bu kılavuzdaki diğer ilkelerle çelişmemek koşuluyla, şifreli mesajlara ve kişilerin gizli anahtarlarına yasal erişimi öngörebilir.

Yasal Sorumluluk: Kriptografik hizmeti veren ve açık/gizli anahtarları dağıtma yetkisi taşıyan kuruluşların yasal sorumlulukları açıkça belirlenmelidir.

Uluslararası Eşgüdüm: Ulusal ve uluslararası politikalar, birbirleriyle eşgüdüm içinde oluşturulmalıdır.

Şifreleme/Deşifreleme (encryption-decryption): Bir bilgisayar ağında veya kişisel bilgisayarlarda haberleşme ya da dosya güvenliğini sağlamak için kullanılır. Bu nedenle günümüzde bilgisayarlarda ya da bilgisayar ağlarında şifrelemenin önemi gün geçtikçe artmaktadır.

Simetrik Şifreleme (Symmetric Encryption): Symmetric Encryption işlemi, bir veri şifrelenirken (encryption) ve şifresi çözülürken (decryption) iki aşamada da aynı Secret Key'in, yani aynı Şifreleme Anahtarı'nın kullanıldığı şifreleme türüdür. Simetrik şifreleme algoritmalarından olan DES Encryption algoritması projelerimizde kullanılmaktadır. DES algoritması, işlemlerini bitler (0 ve 1) üzerinden yapmaktadır. Veriyi bloklara ayırarak şifreleme yapar. Her blok 64 bitten oluşur. Ve 56 bitlik anahtar kullanır. Aynı anahtarla hem şifreleme hem de deşifreleme yapar.

Projelerde kullanılan bir diğer algoritma ise Üçlü- DES algoritmasıdır. Üçlü-DES, iki tane 56-bitlik anahtar kullanmaktadır. Verilen düz metin önce ilk anahtar kullanılarak DES algoritması ile şifrelenir. İkinci anahtar ile şifrelenmiş metin üzerinde, DES'in çözme algoritması uygulanır. İki kez karıştırılmış mesaj, son olarak ilk anahtar kullanılarak tekrar şifrelenir ve şifrelenmiş metin elde edilir. Bu üç adıma Üçlü-DES denir.

Asimetrik Şifreleme (Asymmetric Encryption): Asimetrik şifreleme yönteminde

verinin encryption aşamasında bir şifreleme anahtarı (Public Key), decryption aşamasında ise başka bir şifreleme anahtarı (Private/Secret Key) kullanılmaktadır.

Asimetrik şifreleme yöntemlerinden olan RSA algoritması projelerimizde kullanılmaktadır. RSA algoritması yeterince büyük ve birbirinden farklı olan iki asal sayının çarpımından oluşan bir base değer elde eder ve diğer anahtar parametreleri de aynı iki asal sayıdan türetir.

Projelerde DES, Üçlü- DES ve RSA algoritmaları kullanılmaya devam edilecektir.

E- İmza Kullanımı: Dijital imza, 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.

Doğal olarak dijital imza güvenilirliği şifrelenmiş olmasından kaynaklanır. Bu sistem, şifrelenmiş verileri gönderen bilgisayar ile bu şifrelemeyi çözebilen alıcı bilgisayar arasında çalışır. Gönderenin şifreleme işlemi ile alıcının doğrulama işlemi verinin güvenli bir kaynaktan geldiğini gösterir. Bu iki taraflı işlem dijital imzayı tamamlar. 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.

Elektronik imza, elle atılan ıslak imza gibi kullanılabildiği için, internette her türlü resmi işlemin, hem zamandan hem de kağıt israfından tasarruf edilerek ve elektronik ortamda arşivlenerek yürütülmesini sağlar. Elektronik imza, kamu kuruluşlarıyla yapılan işlemlerde, bankacılık ve sigortacılık işlemlerinde, e-devlet, e-iş ve e-ticaret uygulamalarında, elektronik posta ve kanun kapsamındaki hukuki işlemlerde kullanılabilir. Elektronik imza ile imzalanmış herhangi bir belge bilgisayar ortamında arşivlendiğinden bulunması için zaman harcanmayacaktır. Böylece depolama maliyetleri de yok denecek kadar az olacaktır.

5. YAPTIRIM

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