KİŞİSEL VERİ ŞİFRELEME VE ŞİFRE GÜVENLİĞİ POLİTİKASI

İÇİNDEKİLER

1. GİRİŞ

1.1. AMAÇ

Bu politikanın amacı DOCUART sistemlerinde yer alan verilerin korunması için hangi durumlarda şifreleme yapılması gerektiğini ve kullanılacak şifreleme teknolojilerini belirleyerek, standart bir kullanım sağlamaktır.

1.2. KAPSAM

Bu politika DOCUART ağına veya sistemlerine erişen tüm kişileri kapsar.

1.3. KISALTMALAR VE TANIMLAR

Çalışan	DOCUART Çalışanı
Gizli (Confidential)/Çok gizli (Highly confidential)	Gizli olarak sınıflandırılan bilgiye çok kısıtlı sayıda ve sadece görevi zaruri kıldığı için yetkilendirilmiş kişiler (personel/ hizmet sağlayıcı) tarafından erişilebilir. Çok gizli olarak sınıflandırılan bilgiye ise ancak zorunlu hallerde ilgili kişi tarafından erişilebilir.
Özel (Restricted)	Özel olarak sınıflandırılan bilgiye sadece şirket içindeki ilgili gruplar ve zorunlu durumlarda hizmet ve ürün sağlayıcılar erişebilir (örneğin satış bilgilerine sadece satış bölümünün erişimi gibi).
Hizmete özel bilgi (Internal)	İlgili olan şirket çalışanlarının erişebildiği genel bilgilerdir (Cihaz kılavuzları, Hizmete Özel etiketli politika ve prosedürler, şirket geneline atılmış e-posta kayıtları gibi)
Herkese açık bilgi (Public)	Herhangi bir sınırlama olmaksızın şirket içi ve dışından herkesin erişebildiği bilgilerdir (Şirket iletişim bilgileri Umuma yönelik pazarlama faaliyetleri ve internet sitesi üzerinden yayınlanan hizmet bilgileri ve genel tarifeler gibi)

Kanun	6698 Sayılı Kişisel Verilerin Korunması Kanunu
Kişisel veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel verilerin işlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi
Kullanıcı/Son kullanıcı	**DOCUART** sistemlerine şifre ile erişim sağlayan kişi
NIST (National Institutes of Standards and Technology)	Amerikan Ulusal Standart ve Teknoloji Enstitüsü. Siber güvenlik alanında standartları belirleyen kurum.
Kurum/Kurumumuz	DOCUART
Özel Nitelikli Kişisel Veri	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler

2. GÖREV DAĞILIMLARI VE SORUMLULUKLAR

DOCUART) bünyesindeki tüm birimler ve çalışanlar, Politika kapsamında alınan teknik ve idari tedbirlerin uygulanması konusunda destek vermekte olup, şifre politikasının belirlenmesinde ve uygulanmasında görev alanların unvanları, birimleri ve görev tanımları aşağıdaki tabloda yer almaktadır.

BİRİM	GÖREV TANIMI
BGYS Yönetim Temsilcisi	Veri şifreleme politikasını oluşturmak, yayınlamak ve güncellemek
Bilgi Teknolojileri Ekibi	Veri sınıflandırmasını yapmak
Bilgi Teknolojileri Ekibi	Veri sınıflandırması onaylamak
Bilgi Teknolojileri Ekibi	Uygulanacak şifreleme algoritmalarını belirlemek
Tüm Birimler	Yayınlanan şifreleme politikasına uygun olarak iş süreçlerini yürütmek
Bilgi Teknolojileri Ekibi	Veri şifreleme politikasına uygun olarak periyodik kontroller gerçekleştirmek, güvenlik testlerini yapmak
EYS Yönetim Temsilcisi	Politika kapsamında yapılacak periyodik gözden geçirmeleri gerçekleştirmek

3. VERİLERİN SINIFLANDIRILMASI

DOCUART) sistemleri içerisinde yer alan verilerin korunması için veriler kritiklik durumuna göre sınıflandırılarak, gizlilik derecesine uygun şifreleme algoritmaları ile korunurlar. Veriler sınıflandırılırken korunacak bilginin önemi ve bu verilerin niteliği esas alınır. Yapılan veri sınıflandırması üst yönetim tarafından onaylanır. Üst yönetimin onayı olmadan herhangi bir verinin güvenlik seviyesi daha aşağı seviyeye çekilemez.

6698 sayılı kanun kapsamında işlenen özel nitelikli kişisel verilerin tamamı çok gizli olarak sınıflandırılır.

4. ŞİFRELEME KRİTERLERİ

Veriler yapılan sınıflandırmaya göre şifrelenirken aşağıdaki kriterler uygulanır:

- Gizli veya çok gizli olarak sınıflandırılan veriler şifreli olarak muhafaza edilmelidir.

● Gizli veya çok gizli olarak sınıflandırılan verilerin taşınabilir medya üzerinde muhafaza edilmesi halinde bu medyalar uygun algoritmalar kullanılarak şifrelendikten sonra kilitli kasalarda veya bu tür materyallerin muhafaza için tasarlanan odalarda muhafaza edilmelidir.
● Şifreleme için yalnızca güvenilirliği ispatlanmış, standart algoritmalar kullanılmalıdır.
● Son kullanıcı şifreleri en geç 6 ayda bir değiştirilmelidir.
● Farklı sistemler için aynı şifreyi kullanılmamalıdır.
● Yeni şifre bir önceki şifreden farklı olmalıdır.
● İhtiyaca ve teknik yeterliliğe göre hareket halindeki veriler ve hareketsiz veriler için farklı algoritmalar kullanılmalıdır.
● Kullanılacak şifrelemenin ne kadar güçlü olacağı kullanılan algoritmaya, sistem yeterliliğine ve korunacak verinin türüne göre değişse dahi, NIST (National Institutes of Standarts and Technology) tarafından tavsiye edilen standartlar kullanılmalıdır.
● Şifreleme için kullanılan anahtarların uzunluk gereklilikleri ve kullanılan algoritmaların yeterliliği en az yılda bir kez gözden geçirilmelidir. Kullanılan herhangi bir endüstri standardının değişmesi halinde gözden geçirme işlemi bir yıllık süre beklenmeden gerçekleştirilmelidir.
● Herhangi bir şifreleme algoritması yetkili bilgi güvenlik uzmanları tarafından gözden geçirilip, onaylanmadan kullanılmamalıdır.
● Çok gizli, gizli ve özel nitelikteki verilerin şifrelenmesi için şifreleme algoritmaları yerine şifre kullanılmamalıdır.
● Yetkili kurum ve kuruluşlarca kullanımı kısıtlanmış olan şifreleme algoritmaları kullanılmamalıdır.
● Mümkün olması halinde hizmete özel bilgiler şifre ile saklanmalıdır.

5. ŞİFRELEMENİN İSTİSNALARI

Bu politika kapsamında olmasına rağmen şifrelenmeyecek verilerin Bilgi Teknolojilerinin onaylaması ve Risk Yönetiminin bir parçası olarak şifrelenene kadar periyodik olarak gözden geçirilmesi gerekmektedir.

6. ŞİFRE KORUMA KURALLARI

Mümkün olduğu takdirde yukarıda yer alan şifre oluşturma kurallarına uyulması sistem tarafından kontrol edilir. Şifre güvenliği için aşağıdaki teknik ve idari tedbirler uygulanır:

- Şifrenin 3 kez yanlış girilmesi halinde kullanıcı hesabı kilitlenir. Açılması için müşteri hizmetlerine ulaşması gerekir.
- Aynı kullanıcı adı ve şifre ile eş zamanlı olarak iki farklı hesap kullanılmamalıdır.
- Kullanıcı şifreleri sistemler üzerinde düz metin (plaintext) olarak saklanmaz. Şifreler güçlü şifreleme algoritmaları kullanılarak ve hash değerleri ile saklanır.
- Şifre değiştirme talebin yalnızca ilgili hesap sahibinden gelmesi halinde gerçekleştirilir.
- Sistem üzerinden şifre değiştirme işlemi gerçekleştirilecek kullanıcının öncelikle mevcut şifresi ile sisteme girmesi gerekmektedir.
- VPN veya güvenli ağ bağlantısı olmadan şifreler kullanılarak uzak erişime izin verilmez
- Kritik uzak bağlantılar için çok aşamalı doğrulama kullanılır.

Şifrelerin korunması için alınan teknik ve idari tedbirlerin yanında kullanıcılar, erişim şifrelerini korumak için aşağıdaki kurallara uygun hareket ederler:

- Şifreler üçüncü kişiler ile paylaşılamaz.
- Şifreler yazılı olarak herhangi bir yerde saklanmaz.
- Üst yöneticiler ile şifre paylaşılmaz.
- İşten uzakta olduğunda iş arkadaşları ile şifre paylaşılmaz.
- Uygulamalarda yer alan otomatik şifre kaydetme özelliği DOCUART sistemlerine erişim şifreleri için kullanılmaz.

7. ÇOK AŞAMALI KİMLİK DOĞRULAMA KULLANILMASI

DOCUART gerekli gördüğü durumlarda kullanıcıların şifre ile birlikte ikinci bir doğrulama alt yapısı kullanılmasını zorunlu hale getirebilir. Çok aşamalı kimlik doğrulama kullanılmasına karar verildiğinde bu politikadaki şifre oluşturma ve değiştirme kuralları yeniden gözden geçirilir.

8. ŞİFRELERİN ELE GEÇİRİLMESİ, UNUTULMASI

Kullanıcılar şifrelerinin üçüncü kişilerce ele geçirildiğini fark ettiklerinde derhal şifrelerini değiştirirler. Bu şifre veya benzer şifreleri kullandıkları tüm sistemlerdeki şifrelerini de değiştirirler ve durumu sistem yöneticisine raporlarlar.

Şifrelerin unutulması halinde sistem üzerinden şifre değişikliğinin mümkün olmaması halinde, şifre değişikliğinden sorumlu personele yapılacak başvuru ile şifre değişikliği gerçekleştirilir. Yapılan değişikliklere ilişkin kayıtlar saklanır.

9. POLİTİKANIN UYGULAMASININ TAKİBİ

9.1. ŞİFRELERİN İPTALİ

İşten ayrılan personelin kullanıcı hesapları ve şifreleri vakit geçirmeksizin silinir. İşten ayrılan personelin işten ayrılış işlemleri sırasında kullanıcı hesapları kapatılır ve şifreleri silinir.İnsan kaynakları birimince aylık periyotlarla sonraki ay içerisinde görev değişikliği gerçekleşecek veya işten ayrılacak personelin listesi oluşturularak şifre iptalinden sorumlu personele iletilir. Listede yer alan personelin kullanıcı hesapları ve şifreleri süresi geldiğinde silinir veya kullanımı engelleyecek şekilde pasif hale getirilir.Herhangi bir sisteme erişimine ihtiyaç kalmayan personelin bu sisteme erişim için kullandığı şifreler silinir.

DOCUART tarafından Single Sign On (SSO) kullanımını zorunlu hale getirilirse mevcut tüm şifrelerin kullanımı sonlandırılarak, kullanıcıların yeniden şifre oluşturması sağlanır.

9.2 ŞİFRE GÜVENLİĞİNİN TEST EDİLMESİ

İlgili personel 12 ayda 1'lik periyotlarda yapacağı testler ile kullanılan şifrelerin bu politikada belirlenen kriterlere uygun oluşturulup oluşturulmadığını, süresinde değiştirilip değiştirilmediğini kontrol eder. Politikaya uygun olmadığı tespit edilen kullanımlar üst yönetime rapor olarak sunulur. Şifre güvenliğinin testi için üçüncü kişilerden hizmet alınması halinde, test işleminden önce gizlilik sözleşmesi imzalanması sağlanır.

9.3 ŞİFRE GÜVENLİĞİ EĞİTİMİ

Çalışanlar için periyodik olarak şifre güvenliği ve bilgi güvenliği eğitimi düzenlenir. Bu eğitime DOCUART ağına erişim sağlayan tüm seviyedeki ilgililer katılır.

10. POLİTİKANIN UYGULAMASININ TAKİBİ

Bu politikanın uygulanmasından tüm şirket çalışanları yetkileri çerçevesinde sorumludur. Bu politikaya uyulmamasından dolayı herhangi bir veri ihlali yaşanması halinde ortaya çıkacak hukuki sorumluluklarla ilgili olarak DOCUART kusuru oranında ilgili kişiye rücu edebilir. Ayrıca ilgili hakkında iş aktinin feshi de dahil disiplin düzenlemeleri uygulanabilir.

11. POLİTİKANIN YAYINLANMASI, GÜNCELLENMESİ

İşbu politika DOCUART dosya paylaşım alanında erişilebilir şekilde yayınlanır. Bu politika en az yıllık olarak gözden geçirilir ve gerekmesi halinde DOCUART tarafından politika üzerinde güncelleme gerçekleştirilir. Dokümanın güncel versiyonu DOCUART dosya paylaşım alanında yayımlanır ve ilgililere bilgi verilir. Yapılan değişikliği ilişkin bilgiler politikanın son bölümünde yer alan sürüm bilgileri alanında açıklanır.