1. AMAÇ

Bu politika, Karamanoğlu Mehmetbey Üniversitesi bünyesinde kullanılan/kullanılabilecek kullanıcı adı ve şifre ile erişim sağlanan sistemlerin güvenliği için güçlü bir şifre oluşturulması, oluşturulan şifrenin korunması ve şifre değiştirme sıklığı hakkında standart oluşturmayı amaçlar.

2. KAPSAM

Bu politika Karamanoğlu Mehmetbey Üniversitesinde kullanıcı adı ve hesabı olan (bilgisayar ağına erişen) tüm kullanıcıları kapsamaktadır.

3. SORUMLULAR

- Karamanoğlu Mehmetbey Üniversitesi tüm kullanıcıları.
- Bilgi İşlem Daire Başkanlığı

4. TANIMLAR

CAPTCHA; Ben robot değilim. Kişi doğrulama uygulaması.

5. UYGULAMA

1.1 Genel Şifre Oluşturma Kuralları

- Şifreler teslim alındıktan sonra değiştirilmelidir.
- Şifreler en az 8 karakter uzunluğunda olmalıdır.
- Şifreler en az 5 küçük harf, en az 2 rakam ve en az 1 özel karakter(+,-,*,/) içermelidir.
- Şifre oluştururken aile fertlerinin isimleri kullanılmamalı.
- Şifre oluştururken ardışık sayı ve harf dizileri kullanılmamalıdır.

1.2 Sistem Şifre Oluşturma Kuralları

- Tüm kullanıcı hesaplarına ait bir şifre vardır.
- Yeni kullanıcı hesaplarına ait şifrelerin ilk kez giriş yapılırken kullanıcı tarafından kurallara uygun olarak tanımlanması gerekir.
- Başarısız şifre denemeleri üst üste 5 kere ile sınırlandırılmıştır. Beşinci denemeden sonra şifre ve bağlı olduğu kullanıcı, kullanım dışı bırakılır. Yenilenmesi / kullanım dışılığın açılması için ilgili sistemin yöneticisine telefonla başvurması ve kendisine sorulan (TC kimlik, kurum sicil gibi.) sorulara cevap vermesi beklenir.
- Bilgi kaynaklarına başarılı ve başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerinin kaydı tutulur.
- Personel kendisine verilen kullanıcı bilgileriyle aynı anda 5 cihazdan internete erişebilir.
- Öğrenciler ise kendilerine verilen kullanıcı bilgileriyle sadece 1 cihazdan internete erişebilir.
- Bot ve kaba kuvvet saldırılarını engellemek amacıyla güvenlik kodu doğrulaması veya captcha kullanılmaktadır.
- Yazılan şifrenin ekranda görünmemesi veya maskelenerek görünmesi sağlanır.

1.3 Genel Şifre Kullanım Kuralları

Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde kullanılan şifreler kurum dışında herhangi bir şekilde kullanılmamalıdır, kimse ile paylaşılmamalıdır. İlgili şifreler kuruma ait gizli bilgiler olarak düşünülmelidir.

- Hiç kimse ile şifre hakkında konuşulmamalıdır.
- Aynı şifre birden fazla sistemde kullanılmamalıdır.
- Herhangi bir kişiye telefonda şifre verilmemelidir.
- E-posta mesajlarında şifre belirtilmemelidir.
- Şifreleri en geç 3 ayda bir değiştirilmelidir.
- Değiştirilen şifreler son kullanılan 3 şifreden farklı olmalıdır.
- Şifrenin klavyeden girilmesi sırasında dikkatli olunmalı çevredeki kişilerin görmeyecek şekilde girilmeli.
- İnternet tarayıcıların "şifre hatırla" seçeneği kullanılmamalı. Bunun bir güvenlik açığı olduğu bilinmeli.

1.4 Şifrenin Unutulması

- Bütün sistemler üzerinde kullanıcıların şifrelerin unutma ihtimaline karşı çözüm sistemi olmalıdır.
- Bu çözüm sistemi kullanıcıların kişisel doğrulamasını yapmak amacıyla kişilerin özel bilgi ve kimlik bilgilerinden oluşan en az üç soru içermelidir.
- Çözüm sisteminden şifresini değiştiremeyen kullanıcı Bilgi İşlem Daire Başkanlığı'na gelerek ıslak imza ile yeni şifresini alabilir.
- Kullanıcı şifresi ilgili sistem yöneticisinin onayı olmadan diğer yetkili kişiler tarafından değiştirilmemelidir.
- Bütün şifre değiştirme ve güncelleme işlemleri ayrıca kayıt altına alınmalı kullanıcı, eski ve yeni şifrenin kriptolu hali, değiştiren kişi (kullanıcıdan farklıysa) değiştirme saat ve tarihi korunmalıdır.

1.5 Şifreleme Kontrollerinin Kullanımı

Şifreleme ihtiyaçlarının, yönteminin, gerekli iş alanlarının ve kullanımının belirlenmesi için risk değerlendirmeleri gerçekleştirilir. Çok gizli ve gizli bilgilerin güvenliğinin sağlanması için uygun şifreleme kontrollerinin kullanılması sağlanır. Çok gizli ve gizli bilginin tanımı, ilgili bilginin sahibinin bilgi sınıflandırma sürecine göre vereceği karara bağlıdır. Aktif olarak kullanılmayan gizli bilginin, elektronik saklama ortamlarında (sunucular, manyetik teypler, CD veya taşınabilir bellekler gibi) muhafaza edildiğinde ya da taşındığında, mümkün olan her durumda şifrelenmesi esastır. Uzaktan erişimlerin doğrulanması için kullanılan bilgi uygun şeklide korunur. Statik ya da yeniden kullanılabilir kimlik doğrulama bilgisi, saklanması ya da ağ üzerinden iletilmesi gerektiğinde şifreleme yazılımı ya da donanımı kullanılarak şifrelenmesi tercih edilir.

1.6 Anahtar Yönetimi

Şifreleme algoritmasının tipi ve seviyesi, üzerinde çalışılan kurum bilgisinin kritikliğine göre tayin edilir. Şifreleme anahtarlarının uzunluğu sözleşme gereksinimlerine, yasal yükümlülüklere ve güvenlik ilkelerine uygundur. Şifreleme anahtarları ağ üzerinden iletilemez. Şifreleme sürecinin yönetilmesi için kullanılan anahtarların ağ üzerinden iletilmesi gerekiyorsa, iletim güvenli haberleşme kanalları üzerinden gerçekleştirilir. Sistemler üzerinde şifreli olarak bulunan verilerin şifreleme anahtarları güvenli alanlarda muhafaza edilir ve şifreleme yapan personel haricinde bir personel ya da yöneticinin gereken durumlarda anahtara erişimi sağlanır.

6. İLGİLİ DOKÜMAN

- Şifreleme Prosedürü
- Ağ Güvenliği Politikası
- Ağ Güvenliği Prosedürü