	ŞİFRE POLİTİKASI		
Doküman No: PLT.06	**Yayın Tarihi:** 25.04.2022	**Revizyon Tarihi:** -	**Revizyon No:** -

1. AMAÇ

Bu politikanın amacı şifre oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkında standart oluşturmaktır.

2. KAPSAM

Bu politika kullanıcı hesabı olan sistem ve uygulamalarının şifreleme yöntemlerini kapsamaktadır.

3. KISALTMALAR

Bu prosedürde geçen;

3.1. MSKÜ: Muğla Sıtkı Koçman Üniversitesi'ni ifade eder.

4. TANIMLAR

4.1. Güçlü Şifre: Küçük ve büyük karakterlere sahip hem dijit hem de noktalama karakterleri ve ayrıca harflere sahip, en az sekiz adet alfa-numerik karaktere sahip olan şifredir.

4.2. Zayıf Şifre: Sadece küçük karaktere sahip, sadece harf veya rakamdan oluşan, kişisel bilgi içeren ve sekiz adet karakterden az olan şifredir.

5. SORUMLULUKLAR

MSKÜ'nün bilişim alt yapısını kullanan tüm kullanıcıları kapsamaktadır.

6. UYGULAMA

Şifre bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. Kurum çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifre belirlemekle sorumludurlar.

6.1. Genel Şifre Güvenliği

a) Bütün sistem seviyeli şifreler (örnek, root, administrator) en az yılda bir kere değiştirilmelidir.
b) Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web vs.) en az yılda bir kere değiştirilmelidir.
c) Herhangi bir kişiye telefonda şifre verilmemelidir.
d) Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
e) Üst yöneticiye veya diğer birim personellerine şifreler söylenmemelidir.
f) Kullanıcı, şifresini başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazmamalıdır.
g) Bir kullanıcı adı ve şifresi aynı anda birden çok bilgisayarda kullanılmamalıdır.

Hazırlayan Bilgi Güvenliği Ekibi	Kontrol Eden Bilgi İşlem Daire Başkanlığı	Onaylayan Rektör Yardımcısı

h) Kablosuz bağlantı için kısa süreli misafirlere misafir ağında geçici süreli kullanıcı şifresi oluşturulur. Uzun süreli misafirler (görevli gelenler) için kurumsal kullanıcı adı ve şifresi ile kurumsal hesap oluşturulur ve personel güvenliği ve diğer politikalara uygun davranmakla yükümlüdür.

6.2. Bilgi İşlem Sistemleri Şifre Güvenliği

a) Bütün sistem seviyeli şifreler (örnek, root, administrator) yılda en az bir kere değiştirilmelidir.
b) Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
c) Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.
d) Yönetici erişim şifreleri kapalı bir zarfta imzalı olarak Kurum kasasında saklanmalı ve gereksiz yere açılmamalıdır. Zarfın açılması durumunda Kurum yetkilileri de bilgilendirilmelidir.

6.3. Genel Şifre Oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, Web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vb. bütün kullanıcılar güçlü bir şifre seçimine özen göstermelidir.

Güçlü şifreler aşağıdaki karakteristiklere sahiptir;

a) Küçük ve büyük karakterlere sahiptir (A -Z, a-z).
b) Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir (0 - 9,!,@,&=(,}?,\).
c) En az sekiz adet alfa-numerik karaktere sahiptir.

Zayıf şifreler aşağıdaki karakteristiklere sahiptir;

a) Şifreler sekizden daha az karaktere sahiptir.
b) Şifreler sözlükte bulunan bir kelimeye sahiptir.
c) Şifreler aşağıdaki gibi ortak değere sahiptir:
- Kişinin şahsi bilgilerini içeren kelimelerden oluşur (Adı, soyadı, doğum tarihi, aile fertlerinin isimleri veya baş harfleri, tuttuğu takım, evlilik yıldönümü vb.),
- Bilgisayar terminolojisi, isimleri ve komutlardan oluşur,
- "universite" , "Muğla Sıtkı Koçman" , "MSKÜ" gibi kurumla eşleşebilecek kelimelerden

oluşur,

- AaaBb, qwerty, qazwsx, 123321 gibi sıralı harf veya rakamlardan oluşur.

6.4. Şifre Koruma Standartları

Kurum bünyesinde kullanılan şifreler kurum dışında herhangi bir şekilde kullanılmamalıdır ve kimse ile paylaşılmamalıdır. İlgili şifreler Kuruma ait gizli bilgiler olarak düşünülmelidir. Değişik sistemler için farklı şifre kullanılmalıdır.

a) Herhangi bir kişiye telefonda şifre vermek,
b) E-posta mesajlarında şifre belirtmek,
c) Üst yöneticiye şifreleri söylemek,
d) Başkaları önünde şifreler hakkında konuşmak,
e) Aile isimlerini şifre olarak kullanmak,
f) İş yerinde bulunulmadığı durumlarda iş arkadaşlarına şifreleri bildirmek,
g) Uygulamalardaki "şifre hatırlatma" özelliklerini seçmek.

Yukarıda belirtilen eylemlerin kesinlikle yapılmaması gerekmektedir.

6.5. Yaptırım

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri, tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

7. İLGİLİ DOKÜMANLAR

-