

PAROLA KULLANIMI YÖNERGESİ

1. AMAÇ :

Bu doküman, Afyon Kocatepe Üniversitesi bünyesinde kullanılan bütün parolaların oluşturulması sırasında uyulması gereken kuralları tanımlamak için hazırlanmıştır. Bu kuralların amacı, kullanıcıların ve kurumun, kötü amaçlı saldırılardan korunması ve kişilik haklarının ve kurum kaynaklarının korunmasıdır.

2. KAPSAM:

Bu doküman, Afyon Kocatepe Üniversitesi'nin bilgi teknolojilerinde, parola ile korunan veya korunması gereken bütün bilişim kaynaklarını (yazılım, donanım, hizmet veya kullanıcı vb.) kapsar.

3. SORUMLULAR:

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanlığı sorumludur.

4. KURALLAR:

4.1 Parola oluşturma

4.1.1 Parolalar en az 8 karakter uzunluğunda olmalıdır ve bu karakterlerin en az 1 tanesi sayılardan oluşmalıdır.

4.1.2 Aşağıdaki karakterlerin en az birini içermelidir.

- Büyük harf, (örn. ABCDEF...)
- Küçük harf, (örn, abcdef ...)
- Rakam, (örn: 1234567890)
- Noktalama işareti (örn: !?., vb.) veya özel karakterler (örn: @€+- vb.)

4.1.3 Parolalar aşağıdaki şekilde oluşturulmamalıdır;

- İçeriğinde, kişisel bilgiler bulunmamalıdır (örneğin aile bireylerinin isimleri, doğum tarihleri, telefon numarası veya adres bilgileri gibi)
- Kelime veya rakam dizileri kullanılmamalıdır. (Örn; aaabbb, qwerty, zyxwvuts, 12345678, 123321, vb.)

4.2 Parola yönetimi

4.2.1 Yeni kullanıcı hesaplarına ait parolaların ilk kez giriş yapılırken kullanıcı tarafından kurallara uygun olarak tanımlanması sağlanır.

4.2.2 Başarısız parola denemeleri üst üste 5 kere ile sınırlandırılmıştır. Beşinci denemeden sonra hesap belirli bir süre devre dışı bırakılır.

- 4.2.3 Yazılan parolanın ekranda görünmemesi veya maskelenerek görünmesi sağlanır.
- 4.2.4 Kullanıcı parolaları, saklandıkları ortamlarda, geri dönüşü mümkün olmayan bir şekilde formatı değiştirilerek korunmalıdır (örneğin Hash yöntemi). Bu şekilde en yetkili kişilerin bile parolaları görmesi engellenir.
- 4.2.5 Halka açık veya paylaşılan ağlardan iletilen kimlik bilgileri güçlü şifreleme metotları ile (SSL) korunmalıdır.
- 4.2.6 Başkaları tarafından öğrenildiğinden şüphelenilen parolalar hemen değiştirilmelidir.
- 4.2.7 Kullanıcılar hesaplarını 6 ay içinde kullanmamaları durumunda ilgili hesap dondurulmalıdır.

4.3 Parola kullanımı

- 4.3.1 Parolalar en geç 6 ayda bir değiştirilmelidir.
- 4.3.2 Her yeni parola için, son kullanılan 3 paroladan farklı yeni bir parola kullanılmalıdır.
- 4.3.3 Parolalar hiç kimse ile paylaşılmamalıdır.
- 4.3.4 Parolaların klavyeden girilmesi sırasında dikkatli olunmalı ve çevredeki kişilerin görmesine izin vermeyecek şekilde girilmelidir.
- 4.3.5 E-posta yoluyla parolaların onaylanması veya güncellenmesi istenmez, bu yönde gelen epostalar dikkate alınmamalıdır.
- 4.3.6 Herhangi bir kullanıcının parolası bilerek veya bilmeyerek bir kişi tarafından öğrenilirse, ilgili kullanıcı uyarılmalıdır. Gerekirse zarar verme ihtimaline karşı parolanın kullanıldığı sistem yöneticisi uyarılmalıdır.
- 4.3.7 Aynı parola birden fazla kaynakta kullanılmamalıdır.
- 4.3.8 Parolalar ilave bir şifreleme metodu kullanılmadan hatırlamak amacıyla kayıt edilmemelidir (kâğıt, bilgisayardaki bir dosya, cep telefonu gibi ortamlarda saklanmamalıdır).
- 4.3.9 İnternet tarayıcılarında (internet explorer, chrome, firefox vb.) "Parolayı hatırla" seçeneğinin kişisel bilgisayarlar dışında kullanılmaması, kişisel bilgisayarlarda ise bunun bir güvenlik açığı olduğu hatırlanmalıdır.

4.4 Parolanın unutulması

- 4.4.1 Bütün sistemler üzerinde, kullanıcıların parolasını unutma ihtimaline karşı bir çözüm sunulmalıdır.
- 4.4.2 Bu çözüm, kullanıcıların kişisel doğrulamasını yapmak amacıyla kişilerin gizli soruları ve özlük bilgilerinden oluşan en az iki soru içermeli veya daha önce kişinin kendisinden alınan alternatif mail adresi ile yapılmalıdır.

4.4.3 Hiçbir kullanıcının parolası kullanıcının talebi olmadan (yasal durumlar harici) ve yönetim birimlerinin onayı olmadan yetkili kişiler tarafından değiştirilmemelidir.