	POLİTİKA	**DOKÜMAN NO**	BGYS.PLT.02
		YAYIN TAR.	25.03.2025
		REVİZYON NO	03
		REVİZYON TARİHİ	12.03.2025
KONU	AFYON KOCATEPE ÜNİVERSİTESİ PAROLA POLİTİKASI		

Revizyon Takip Tablosu		
Revizyon No	**Revizyon Tarihi**	**Revizyon Nedeni**
2	06.03.2023	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi uyum çalışmaları kapsamında değişikliğe gidilmiştir.
3	21.11.2023	ISO27001:2022 standardına uyum

1. AMAÇ

(1) Bu Politikanın amacı, Afyon Kocatepe Üniversitesi bilgi sistemlerinde kullanılan parolaların güçlü bir şekilde oluşturulmasına, korunmasına, değiştirilmesine ve değiştirilme sıklığına yönelik politikalar ile usul ve esasları düzenlemektir.

2. TANIMLAR

(1) Bu Politikada geçen;

a) Kullanıcı: Afyon Kocatepe Üniversitesinin tüm personelini, Afyon Kocatepe Üniversitesine kayıtlı öğrenciyi veya geçici olarak üniversite bünyesinde bulunan kişiyi,

b) Kurum: Afyon Kocatepe Üniversitesini,

ifade eder.

3. KAPSAM

(1) Bu Politika, kurumdaki bilgi sistemlerinde kullanılan parolaların güçlü bir şekilde oluşturulmasının, korunmasının, değiştirilmesinin ve değiştirilme sıklığının, bu Politikaya ve ilgili diğer mevzuata uygun olmasına ilişkin politikalar ile usul ve esasları kapsar.

4. POLİTİKALAR

1. (1) Kurumdaki bilgi sistemlerinde kullanılan parolalar ile ilgili ilkeler şunlardır:

a) İlk parola gönderimi sırasında rastgele parola üretilir.
b) Başkaları tarafından öğrenildiği veya ele geçirildiği tespit edilen veya bundan şüphelenilen parolalar, kurum tarafından hemen değiştirilir.[2]
c) Parolalar en az sekiz karakterden oluşmalı, en az bir büyük harf, bir küçük harf, bir rakam ve bir özel karakter içermelidir.[4]
ç) Kullanıcılar, merkezî kimlik doğrulaması yapılmayan her sistem için farklı parolalar kullanmalıdır.[6]
d) Kimlik doğrulama için kolay erişilebilecek bilgi sorgulayan sorular ve cevaplar kullanılmamalıdır.[8]
e) Üst üste başarısız parola denemesi olması hâlinde kullanıcı hesabı belirli bir süre devre dışı bırakılır.[9]
f) Sistem yöneticileri “Administrator” ve ”root” gibi genel sistem hesaplarını kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır. Ancak zorunlu hallerde “root” veya “admin” vb. yetkili kullanıcılarla bağlanılmalıdır. Root veya admin şifresi, sadece sistem yöneticilerinde bulunmalıdır.[7]
g) Taşınabilir cihazlarda kullanılan veya cihaz üzerine sabitlenen sistemlerde parola haricinde PIN belirlenmelidir.[10]

5. USUL VE ESASLAR

(1) Kurum bilgi sistemlerinde kullanılan parolaların oluşturulması ve saklanması ile ilgili usul ve esaslar şunlardır:

a) Kullanıcılar güçlü bir parola oluşturmalıdır. Sistem tarafından oluşturulan parolalar ise ilk girişten sonra kullanıcı tarafından güçlü bir parola olacak şekilde değiştirilmelidir.

b) Güçlü parola veya parola haricinde belirlenmesi gereken PIN aşağıdaki özelliklere sahip olmalıdır:

1) En az bir küçük ve bir büyük harf, rakam ve noktalama karakteri içermelidir. (Örneğin: A-Z, a-z, 0-9,!,@,&=(,}?,\)

2) Parolalar herhangi bir yere yazılmamalı ve elektronik ortamda tutulmamalıdır.

3) Parola giriş alanları uzun ve karmaşık bir parola girilmesini engellememeli, parola cümle (deyimsel parola) kullanımına izin vermeli ya da teşvik etmelidir.

4) Parolalar, kişi veya kamu için önemli tarihleri, kişinin tuttuğu spor takımı, memleketi veya yaşadığı yer ile ilgili bilgileri ve buna benzer kolay tahmin edilebilir bilgileri içermemelidir.

(2) Kurum bilgi sistemlerinde kullanılan parolaların korunması ile ilgili usul ve esaslar şunlardır:

a) Kurum bilgi sistemlerinde kullanılan parolaların aynısı veya benzeri kurum dışında herhangi bir şekilde kullanılmamalıdır.

b) Parolalar, kimse ile paylaşılmamalıdır.

c) Değişik bilgi sistemleri için farklı parolalar kullanılmalıdır.

ç) Parolaların çalınmasına yönelik tüm eylemlere karşı tedbirli olunmalıdır.[11]

d) Uygulamalardaki “beni hatırla“ gibi kullanıcı bilgilerini saklayan özellikler seçilmemelidir.[12]

(3) Kurum bilgi sistemlerinde kullanılan parolaların değiştirilmesi ve değiştirilme sıklığı ile ilgili usul ve esaslar şunlardır:

a) Bütün yönetici (root, administrator vb.) ve kullanıcı (e -posta, web vb.) düzeyli parolalar 180 günde bir değiştirilmelidir. Değişim sırasında belirlenecek yeni parola, kullanılan son üç parola ile aynı olmamalıdır. [1]

b) Değişen parola fonksiyonu eski parolayı, yeni parolayı ve bir parola onayını kapsamalıdır.

c) Parola değişim süresi gelen hesaplar ilk oturum açmadaki başarılı işlem sonrasında doğrudan parola değişim ekranına yönlendirilir. Parola değişim işlemi gerçekleştikten sonra kullanıcı, oturum açma ekranına tekrar yönlendirilir.

ç) Kullanıcı, ilk parola gönderimi sırasında rastgele üretilen parolayı sisteme giriş sırasında değiştirmeye zorlanır.

d) Tüm varsayılan parolalar, sistem kullanılmaya başlamadan önce kullanıcı veya sistem/ağ yöneticileri tarafından değiştirilecektir. Bilgisayarlara ilk tanımı yapılan kullanıcı için; kullanıcı sisteme giriş yapıldığında parolasının değiştirmesi sağlanacaktır.[7]

6. YAPTIRIM

(1) Bu Politikaya aykırı hareket eden kullanıcılar hakkında mevzuatta belirtilen hükümler ve disiplin prosedürü uygulanır.

Hazırlayan	Kontrol Eden	Onaylayan
BGYS Yöneticisi	BGYS Üst Yönetim Temsilcisi (Bilgi İşlem Daire Başkanı)	Üst Yönetici (Rektör)