



TRK-ALMAN NİVERSİTESİ

PAROLA POLİTİKASI

Revizyon Takibi:

Sıra No	Rev. No	Tarih	Hazırlayan	Revizyon Nedeni	Onaylayan	İmza
1						
2						
3						
4						

	POLİTİKA	Doküman No	TAU-POL.119
		Yürürlük Tarihi	09.04.2026
		Revizyon No / Tarih	00
		Gizlilik Derecesi	Hizmete Özel
		Sayfa No	2 / 4
DOKÜMAN ADI	PAROLA POLİTİKASI		

1. AMAÇ

Bu politikanın amacı, Türk-Alman Üniversitesi bilgi sistemleri altyapısında yer alan bilgisayar sistemleri, elektronik posta, internet ve diğer erişimler için güçlü parola oluşturmak ve parolalarla ilgili diğer işlemleri düzenlemektir. Politika, başta Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi 3.2.1.8 maddesine ve ilgili diğer maddelere dayalı güvenlik tedbirlerine uygunluğu hedeflemektedir.

2. KAPSAM

Bu politika, Türk-Alman Üniversitesi bünyesindeki tüm çalışanları ve bilgi sistemlerini kapsar.

3. SORUMLULUK

Bu prosedürün uygulanmasından Yönetim Temsilcisi başta olmak üzere tüm personel sorumludur.

4. UYGULAMA

4.1. Genel Kurallar

- Bilgisayar sistemlerine ve tüm parola gerektiren uygulamalara boş parola ile erişmek mümkün olmayacaktır.
- Parolalar gizli bilgidir. Kişiye özel (tekil) olmak üzere oluşturulmalıdır.
- Parolalar güçlü olmalıdır.
- Bütün kullanıcı seviyeli parolalar (örnek, e-posta, web vb.) en az 180 günde bir değiştirilmelidir.
- Sistem yöneticisi farklı sistemler için farklı parolalar kullanmalıdır.
- Kullanıcı yönetimi Active Directory üzerinden yapılmaktadır.
- Parolalar e-posta iletileri ile gönderilmemelidir.
- Kullanıcıya bildirilecek parolalar güvenli bir ortamda iletilmelidir.
- Parolalar hatırlamak maksadı ile kâğıt ortamına yazılmamalı ve görülecek mekânlara, açık bir şekilde masalara, monitör üstlerine konulmamalıdır.
- Parolalar başka kişilerle paylaşılmamalıdır.
- Herhangi bir parola bilgisayar sistem dosyalarında düz metin olarak tutulmamalıdır.
- Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının parolaları da kolayca kırılmayacak güçlü bir parolaya sahip olmalıdır.
- Tüm varsayılan parolalar, sistem kullanılmaya başlamadan önce kullanıcı veya sistem/ağ yöneticileri tarafından değiştirilecektir. Bilgisayarlara ilk tanımı yapılan kullanıcı için; kullanıcı ilk sisteme login olduğunda parolasını değiştirmesi sağlanacaktır.
- Sistem kullanıcıları aynı zamanda birden çok kullanıcı tarafından kullanılmamalıdır. Mümkün olmayan durumlarda kullanıcı hareketleri loglanarak takip edilmektedir.

	HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Unvanı	Bilgi Güvenliği Ekip Üyesi	Bilgi Güvenliği Ekip Üyesi	Bilgi Güvenliği Yöneticisi
Adı Soyadı	Elif İNDR	Zeynep KÜÇÜK	Sümeyya SONGUR

	POLİTİKA	Doküman No	TAU-POL.119
		Yürürlük Tarihi	09.04.2026
		Revizyon No / Tarih	00
		Gizlilik Derecesi	Hizmete Özel
		Sayfa No	3 / 4
DOKÜMAN ADI	PAROLA POLİTİKASI		

4.2. Genel Parola Oluşturma Kuralları

Parolalar değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: kullanıcı parolaları, web erişim parolaları, e-posta erişim parolaları, ekran koruma parolaları, yönlendirici erişim parolaları vb. Bütün kullanıcılar güçlü bir parola kullanmalıdır.

Güçlü Parolalar aşağıdaki karakteristiklere sahiptir.

- Küçük ve büyük karakterlere sahiptir (A -Z, a-z).
- Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir (0 - 9,!,@,&=,}?,\).

Domaine dâhil edilen, iş amacıyla personele tahsis edilmiş olan istemcilerde, kullanıcı hesap parolaları aşağıdaki minimum gereksinimleri karşılamalıdır:

- İlk oturum açma esnasında personelin aşağıda belirten parola politikasına uygun bir parola belirlemesi zorunlu tutulmaktadır.
- Kullanıcının hesap adını veya kullanıcının esas adını içermemelidir.
- En az sekiz karakter uzunluğunda olmalıdır.
- Aşağıdaki dört kategorinin en az üçünden karakterler içermelidir:
 - Büyük harfli karakterler (A'dan Z'ye kadar)
 - Küçük harfli karakterler (a'dan z'ye kadar)
 - Rakamlar (0- 9 arası)
 - Alfabetik olmayan özel karakterler (!, \$, #, %, @)
- 180 günde bir değiştirilmelidir.
- Değiştirildikten sonra en az bir gün kullanılmalıdır.
- Kullanılan son üç parola haricinde bir parola belirlenmelidir.
- Parolanın unutulması durumunda ilgili sistem yöneticisine başvurulmalıdır.

4.3 Genel Parola Koruma Standartları

- Kurum bünyesinde kullanılan parolalar kurum dışında herhangi bir şekilde kullanılmamalıdır.
- Kimse ile paylaşmayınız. İlgili Parolalar kuruma ait gizli bilgiler olarak düşünülmelidir. Değişik sistemler için farklı parola kullanılmalıdır.
- Uygulamalardaki “parola hatırlatma” özellikleri seçilmemelidir.
- Parolalar en az 180 günde bir değiştirilmelidir.
- Parolalar 5 sefer yanlış girildiğinde hesap kilitlenir. 5 dakika boyunca hesap kilitli kalır.
- Parolalarda son 2 parola hatırlanmaktadır. Parola en az 1 gün kullanılmak durumundadır.
- Veri tabanı sunucuları, internet erişim cihazları, anti-virüs programı, toplu e-mail yazılımı erişim parolaları kapalı bir zarfta imzalı olarak kurumun kasasında saklanmalı ve gereksiz yere açılmamalıdır. Zarfin açılması durumunda kurum yetkilileri de bilgilendirilmelidir.
- Kullanıcı parolaların değiştirilip değiştirilmediği Active Directory ile otomatik olarak takip edilir.

Aşağıdaki faaliyetler gerçekleştirilmemelidir:

- Herhangi bir kişiye telefonda parola vermek.

	HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Unvanı	Bilgi Güvenliği Ekip Üyesi	Bilgi Güvenliği Ekip Üyesi	Bilgi Güvenliği Yöneticisi
Adı Soyadı	Elif İNDR	Zeynep KÜÇÜK	Sümeyya SONGUR



POLİTİKA

Doküman No	TAU-POL.119
Yürürlük Tarihi	09.04.2026
Revizyon No / Tarih	00
Gizlilik Derecesi	Hizmete Özel
Sayfa No	4 / 4

DOKÜMAN ADI

PAROLA POLİTİKASI

- E-posta mesajlarında parola belirtmek.
- Üst yöneticinize parolaları söylemek.
- Başkaları önünde parolalar hakkında konuşmak.
- Aile isimlerini parola olarak kullanmak.
- Parolaları işten uzakta olduğunuzda iş arkadaşlarınıza bildirmek.

4.4 Veri Tabanı Parola Oluşturma Kuralları

- Genel parola oluşturma ve saklama kuralları veri tabanı sistemleri için de kullanılacak parolalar içinde aynen uygulanır.

	HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Unvanı	Bilgi Güvenliği Ekip Üyesi	Bilgi Güvenliği Ekip Üyesi	Bilgi Güvenliği Yöneticisi
Adı Soyadı	Elif İNDIR	Zeynep KÜÇÜK	Sümeyya SONGUR