



**SÜLEYMAN DEMİREL ÜNİVERSİTESİ**  
**Bilgi İşlem Daire Başkanlığı**  
**Şifre Güvenliği Politikası**

Doküman No

PLT-003

İlk Yayın Tarihi

22.1.2020

Revizyon Tarihi

10.9.2021

Revizyon No

001

Sayfa No

1 / 3

## 1. AMAÇ

Bu politikanın amacı güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkında standart oluşturmaktır

## 2. KAPSAM

Bu dokümanla Süleyman Demirel Üniversitesi'nin bilgi teknolojilerinde, parola ile korunan veya korunması gereken bütün kaynakları (yazılım, donanım, hizmet veya kullanıcı vb.) kullanıcıları, çalışma alanlarını ve sistem yerleşkelerini kapsar.

## 3. SORUMLULUKLAR

Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre bilgi güvenliğini tümüyle riske atabilir. Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dâhilinde şifreleme yapmakla sorumludurlar.

## 4. UYGULAMA

### 4.1. Genel

- Bütün sistem seviyeli şifreler (örnek, root, administrator) 6 ayda bir değiştirilmelidir.
- Bütün kullanıcı seviyeli şifreler (örnek, e -posta, web vs.) için tavsiye edilen değiştirme süresi 90 günde birdir.
- Şifre değişiklikleri için sistem yöneticisinden destek alınmalıdır.
- Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
- Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.
- Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılmayacak güçlü bir şifreye sahip olmalıdır.
- Bir kullanıcı adı ve şifresi aynı anda birden çok bilgisayarda kullanılmamalıdır.

### 4.2. Ana Noktalar

#### 4.2.1. 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 şifreleridir. Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

- Kullanıcılar giriş yaptıkları bilgisayardan çıktıktan sonra farklı bir bilgisayardan giriş yapabilirler.
- Yazılan parolanın ekranda görünmemesi veya maskelenerek görünmesi sağlanır.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Öğretim Görevlisi - Gözde BİÇEN	Doktor Öğretim Üyesi - Veli ÇAPALI



**SÜLEYMAN DEMİREL ÜNİVERSİTESİ**  
**Bilgi İşlem Daire Başkanlığı**  
**Şifre Güvenliği Politikası**

Doküman No PLT-003

İlk Yayın Tarihi 22.1.2020

Revizyon Tarihi 10.9.2021

Revizyon No 001

Sayfa No 2 / 3

• Kullanıcı parolaları, saklandıkları ortamlarda, geri dönüşü mümkün olmayan bir şekilde bozularak korunur (örneğin Hash), bu sayede en yetkili kişilerin bile kullanıcı parolasını görmesi engellenir. Bilgi kaynaklarına başarılı ve başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerinin kaydı tutulur.

• Kullanıcıların kimlik doğrulaması yaparak oturum açtıkları sistemlerin başından ayrıldıklarında (sisteme parola ile giriş yapıldıktan sonra sistem açık bırakılması halinde) en geç 10 dakika sonra otomatik olarak kapanması (sistemin kilitlenmesi) sağlanır.

• Halka açık veya paylaşılan ağlardan iletilen kimlik bilgileri güçlü şifreleme metotları ile (SSL) korunur.

• Başkaları tarafından öğrenildiğinden şüphelenilen parolalar hemen değiştirilir.

• Kritik kaynaklara 3'lü şifre ile erişilebilir, bu sayede tek bir kullanıcının sistemde güvenlik ihlali oluşturmasına izin verilmez. (örneğin bilgi kaynaklarına erişim kayıtları gibi kayıtlara en yetkili kullanıcı bile tek başına erişemez, bu yetkili kullanıcılardan 3 kişinin oluşturduğu bir heyet kendi şifrelerini aynı anda girerek kritik bilgilere erişebilir)

Güçlü Şifreler aşağıdaki karakteristiklere sahiptir.

- Küçük ve büyük karakterlere sahiptir. (A -Z , a-z)
- Rakam, noktalama karakterleri ve harflere sahiptir.(0 - 9,!,@,&=(,)?,\\)
- En az on adet Alfa numerik karaktere sahiptir.
- Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
- Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır.
- Parolalar 6 ay yaşlanma süresine sahiptir. Kullanıcılar 6 ay sorunda otomatik olarak şifre sıfırlamaya zorlanırlar.

#### 4.2.2 Genel Şifre Koruma Standartları

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

Aşağıdaki faaliyetleri gerçekleştirmek kesinlikle yasaktır.

- Herhangi bir kişiye telefonda şifre vermek
- E-posta mesajlarında şifre belirtmek
- Üst yöneticiye şifreleri söyleme
- Başkaları ile şifreler hakkında konuşmak
- Aile isimlerini şifre olarak kullanmak
- Uygulamalardaki “şifre kaydetme” özelliğinin seçilmesi.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Öğretim Görevlisi - Gözde BİÇEN	Doktor Öğretim Üyesi - Veli ÇAPALI

	<b>SÜLEYMAN DEMİREL ÜNİVERSİTESİ</b> <b>Bilgi İşlem Daire Başkanlığı</b> <b>Şifre Güvenliği Politikası</b>	Doküman No	PLT-003
		İlk Yayın Tarihi	22.1.2020
		Revizyon Tarihi	10.9.2021
		Revizyon No	001
		Sayfa No	3 / 3

#### 4.3. Parolanın Unutulması

- Bütün sistemler üzerinde, kullanıcıların parolasını unutma ihtimaline karşı bir çözüm sunulmuştur.
- Bu çözüm, SDUNET <https://sdunet.sdu.edu.tr> web adresinden parolamı unuttum bölümü kullanılarak kullanıcının cep telefonu ile ikinci bir doğrulama alınarak parolanın sıfırlanmasını içermektedir. Eğer kullanıcının cep telefonu sistemde kayıtlı değilse kullanıcıların Personel Daire Başkanlığına kimlikleri ile başvurarak telefon numarasını ekletmesi ya da düzeltilmesi gerekmektedir.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Öğretim Görevlisi - Gözde BİÇEN	Doktor Öğretim Üyesi - Veli ÇAPALI