# AMAÇ

Bu politikanın amacı, Aydın İl Sağlık Müdürlüğü ve Bağlı Kamu Sağlık Tesisleri bünyesinde çalışan personellerin, tüm bilgi sistemleri uygulamalarında ve kurumsal e-posta hesaplarında kullanılacak olan parolaların üretilmesi, korunması, kullanılması ve değiştirilme sıklığı hakkında kurumsal bir standart oluşturmaktır.

# KAPSAM

Aydın İl Sağlık Müdürlüğü Bilgi Güvenliği Yönetim Sistemi Politika metninde yer alan kapsam maddesinde belirlenmiş olan kapsamdır.

# TANIMLAR

**İSM:** Aydın İl Sağlık Müdürlüğü

**Bağlı Sağlık Tesisleri**: Kamu Hastaneleri, İlçe Sağlık Müdürlükleri, Toplum Sağlığı Merkezleri, Entegre Hastaneler, Halk Sağlığı Laboratuvarı, İl Ambulans Servis Başhekimliği

**Root, Administrator:** Tam yetkili kullanıcı, sistem yöneticisi

**e-posta:** İnternet üzerinden gönderilen elektronik mektup.

1. **SORUMLULUKLAR**

Bu prosedürün uygulanmasından ilgili kurum yöneticileri sorumludur.

# UYGULAMA

* 1. **Parola Yönetimi ve Kullanımı**
		1. Kullanıcılar hesaplarına ait parolaları (örnek: e-posta, web, masaüstü bilgisayar vs.) en geç 6 (altı) ayda bir değiştirmelidir.
		2. Sistem yöneticileri, kendi yönetimindeki sistem ve kendi kullanıcı hesapları için farklı parolalar kullanmalıdır.
		3. Parolalar, e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
		4. Kullanıcı, parolasını başkası ile paylaşmamalı, kağıtlara ya da elektronik ortamlara yazmamalıdır.
		5. Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da **“5.2. Parola Güvenliği”** maddesinde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.
		6. İSM ve Bağlı Sağlık Tesislerinde bütün parolalar gizli bilgi niteliğindedir. Paylaşılamaz, kağıtlara ya da elektronik ortamlara yazılamaz.
		7. Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki **"parola hatırlama"** seçeneği kullanılmamalıdır.
		8. Kullanıcı son 3 parolayı tekrar kullanmamalıdır.
	2. **Parola Güvenliği**
		1. Müdürlüğümüz ve Bağlı Sağlık Tesislerinde kullanılan sistem ve uygulamaların kullanıcıları asgari olarak aşağıdaki kurallara uygun parola kullanmalıdır.
			1. Parolalar en az 8 (sekiz) karakterden oluşur.
			2. Sistem yönetim işlemlerinde kullanılan parolaların (root, administrator, sysadmin vb.) en az 12 karakterden oluşturulmalıdır.
			3. İçerisinde en az 1 (bir) tane büyük ve en az 1 (bir) tane küçük harf bulunur.
			4. İçerisinde en az 1 (bir) tane rakam bulunur.
			5. İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !, ?, A, +, $, #, &, /, {, \*, -, ], =, ...)
			6. Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, ababab, ...)
			7. Sıralı karakterlerin kullanılması engellenir. (abcd, qwert, asdf, 1234, zxcvb, ...)
			8. Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, qwerty, doğum tarihi, çocuğun adı, soyadı gibi)
			9. Sözlükte bulunabilen kelimelerin kullanılması engellenir.
			10. Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

# YAPTIRIM

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla **“Bilgi Güvenliği Disiplin Prosedürü”** dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.