



SAMSUN İL SAĞLIK MÜDÜRLÜĞÜ E-POSTA KULLANIMI VE PAROLA GÜVENLİĞİ KULLANIM POLİTİKASI



1. ELEKTRONİK POSTA (e-posta) GÜVENLİĞİ

1.1. Kurumsal iş ve işlemleri yerine getirmek üzere tüm personellerimiz 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ve Bakanlığımızın resmi yazısı doğrultusunda kurumsal e-posta adreslerini kullanmaları zorunludur.

1.2. Kurumsal olmayan şahsi e-posta adreslerinden (@gmail.com, @yandex.com vb.) kurumsal iletişim yapılmayacak, kurumsal e-posta hesapları (@saglik.gov.tr) şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.

1.3. Kurumsal faaliyetler ile ilgili veriler, veri aktarımı vb. maksatlarla geçici süre için olsa dahi Bakanlığımız kontrolünde olmayan depolama alanlarında (Google Drive, iCloud, Yandex Disk, We Transfer, Rapid Share) bulundurulmayacaktır. Bu amaçla kurum iç ağında tesis edilmiş ve İnternet erişimi olmayan dosya sunucuları ve/veya Bakanlığımız tarafından merkezi bir hizmet olarak işletilen ve <https://sbtransfer.saglik.gov.tr/> adresinden ulaşılabilen dosya paylaşım ortamı kullanılacaktır.

1.4. Mobil uygulamalar (WhatsApp, Massenger, Line, Viber, Telegram, WeChat, Skype, SnapChat vb.) ve sosyal medya platformları (Facebook, Youtube,Instagram,Twitter,LinkedIn vb.) üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.

1.5. KVKK tarafından 6698 sayılı Kanunda yer alan bazı hususların açıklanması amacıyla alınan 2018/10 sayılı karar gereği, e-posta ile aktarılacak verilerin özel nitelikli kişisel veri statüsünde olması durumunda aktarma işlemlerinin kurumsal e-posta veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak yapılması kanuni zorunluluktur.

1.6. Müdürlüğümüzde görev yapan 657 sayılı Kanuna bağlı tüm kamu personeline, talep etmeleri halinde kurumsal e-posta hesabı açılır.

1.7. Çeşitli sözleşmeler kapsamında Müdürlüğümüzde görev yapan ve yaptıkları iş gereği e-posta hesabı olması gereken personele, sıralı yöneticileri tarafından onay verilmesi halinde kurumsal e-posta hesabı açılır.

1.8. Bakanlığımız merkez ve taşra teşkilatında yer alan birimler için ihtiyaç olması halinde, tüzel e-Posta hesapları açılır. Tüzel e-Posta hesapları, ilgili birimin adı veya yürüttüğü işler ile alakalı olarak belirlenir. (bilgiguvenligi@saglik.gov.tr, some@saglik.gov.tr gibi).

1.9. Kurumsal ve tüzel e-Posta hesabı açılması için başvuru usulleri ve ilgililerince yapılacak işlemler Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunda (Merkezi Aktif Dizin ve E-Posta Sistemine Erişim) belirtilmiştir.

1.10. Kurumsal ve tüzel e-Posta kullanım kayıtları Bakanlıkça tutulur. Bu kayıtlar 6698 sayılı Kanun'un 28'inci maddesinin birinci ve ikinci fıkralarında yer alan şartlar kapsamında; yalnızca yetkili kişi, kurum ve kuruluşlar tarafından, yine aynı Kanunun 4'üncü maddesinde yer alan genel ilkelere uymak kaydıyla incelenebilir.

1.11. Bakanlık tarafından uygulanan e-Posta yönetimi ve güvenliği ile ilgili politikalar şu şekildedir:

1.9.1. Kullanıcıların e-Posta hesaplarına tarayıcı programları, masaüstü istemci uygulaması (Office Outlook) ve cep telefonları üzerinden güvenli olarak erişebilmeleri için gerekli servisler sağlanır.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ekrem MORAL Bilgi Güvenliği Yetkilisi	Erol ÖZTÜRK Personel ve Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Dr.Öğr.Üyesi Muhammet Ali ORUÇ İl Sağlık Müdürü



SAMSUN İL SAĞLIK MÜDÜRLÜĞÜ E-POSTA KULLANIMI VE PAROLA GÜVENLİĞİ KULLANIM POLİTİKASI



1.9.2. e-Posta hesabı ilk kez açıldığında kullanıcılara “Bakanlık e-Posta Kullanım Politikası ve e-Posta Kullanımında Dikkat Edilmesi Gereken Hususlar/Kullanıcı Sorumluluklarını Bildiren Bilgilendirme Yazısı” e-Posta ekinde gönderilir.

1.9.3. Kullanıcı parolalarının Bilgi Güvenliği Kılavuzu (Parola Güvenliği) maddesinde belirtilen politikalar ile uyumlu olup olmadığı denetlenir.

1.9.4. Bakanlık e-Posta sistemi tarafından oluşturulan ve sisteme ilk kez girişte kullanılan parolanın ilk kullanımdan sonra değiştirilmesi sağlanır.

1.9.5. Kullanıcıların son kullandığı üç parolayı kullanması engellenir.

1.9.6. Kullanıcılar, altı ayda bir parolalarını değiştirmeye zorlanır. Parola değiştirme süresine beş (5) gün kala uyarı iletisi gönderilir.

1.9.7. Kullanıcılara e-Posta hesabının parolasını değiştirmek için kısa mesaj Bilgi Güvenliği Politikaları Kılavuzu 37 servisi (SMS) ile onay kodu gönderilir veya alternatif e-Posta aracılığı ile parola değişimi sağlanır. SMS onayı kullanıcıyı yeni oluşturacağı parola ekranına yönlendirir. Kullanıcıların daha önce sisteme kaydettiği alternatif e-Posta adresi üzerinden parola yenilenmesi tercih edilmişse, sistem tarafından parola değişikliği linki gönderilir.

1.9.8. 657 sayılı Kanun kapsamı dışında istihdam edilmiş olan personel için e-Posta hesabının ilk açılmasından itibaren aktif dizinde bir yıl kullanım süresi belirlenir. Bir yıllık süre dolduğunda aktif dizin aracılığı ile kimlik doğrulaması yapan tüm uygulamalara erişimler kapatılır.

1.9.9. Bir yıl süre ile sisteme giriş yapmayan kullanıcıların hesapları geçici olarak kapatılır. Bu hesaplar aktif dizinde pasife çekilir.

1.9.10. Kullanıcılara e-Posta hesabı ilk kez açıldığında bir GB disk alanı tanımlanır. Kota artırımı e-Posta Birimi tarafından dinamik olarak veya e-Posta Birimine e-Posta ile yapılan talepler doğrultusunda yapılır.

1.9.11. Yüksek sayıda üye içeren dağıtım gruplarına gönderilen iletilerin denetim ve onay işlemleri için “moderatör” tanımlanır. İhtiyaç olması durumunda sadece belirli kullanıcıların veya grupların söz konusu dağıtım gruplarına ileti göndermesi için detay yetkilendirmeler yapılır.

1.9.12. Yüksek sayıda üye içeren dağıtım grupları, tüm kullanıcılar tarafından görülen genel adres defterinden gizlenir.

1.9.13. Bir e-Postaya eklenebilecek en fazla alıcı sayısı 100 (yüz) e-Posta adresi ile sınırlı tutulur.

1.9.14. Gönderilen e-Posta boyutu 25 MB’yi geçemez.

1.9.15. Dağıtım gruplarının kullanım durumları (e-Posta akış trafiği) takip edilir ve bir yıl boyunca kullanılmayan gruplar tespit edilerek silinir.

1.9.16. e-Posta iletimlerinde “exe” gibi çalıştırılabilir dosyaların gönderilmesi engellenir.

1.9.17. e-Posta sistemlerinde fazla veri (data) boyutu oluşturması sebebi ile e-Posta hesaplarına profil resmi eklenmesi engellenir.

1.9.18. *@saqlik.gov.tr uzantılı e-Posta hesabından farklı uzantılı e-Posta adreslerine gönderilen iletilerde e-Posta Yasal Uyarı (Disclaimer) metni gönderilir.

1.10. Kurumsal ve tüzel hesapların kullanımında dikkat edilmesi gereken hususlar şu şekildedir;

Hazırlayan	Kontrol Eden	Onaylayan
Ekrem MORAL Bilgi Güvenliği Yetkilisi	Erol ÖZTÜRK Personel ve Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Dr.Öğr.Üyesi Muhammet Ali ORUÇ İl Sağlık Müdürü



SAMSUN İL SAĞLIK MÜDÜRLÜĞÜ E-POSTA KULLANIMI VE PAROLA GÜVENLİĞİ KULLANIM POLİTİKASI



1.10.1. Kullanıcılar, kendilerine tahsis edilen e-Posta hesabını bir başka kişiye kullandıramaz veya devredemez.

1.10.2. Kullanıcılar, parolalarını Bilgi Güvenliği Politikaları Kılavuzunda (Parola Güvenliği maddesinde) belirtilen parola politikaları uyarınca oluşturur ve kullanır.

1.10.3. Kullanıcılar, kendilerine ait parolanın güvenliğinden ve söz konusu parola kullanılarak gönderilen e-Postalardan doğacak hukuki işlemlerden sorumludur.

1.10.4. Kurumsal e-Posta hesabı yalnızca kurumsal süreçlere ilişkin iş ve işlemlerde kullanılabilir. Kurumsal e-Posta hesaplarının, idari ve hukuki düzenlemelere aykırı ya da şahsi iş ve işlemlere ilişkin kullanımından kaynaklanan her türlü adli, idari, mali ve cezai sorumluluk ilgili hesap sahibine aittir.

1.10.5. Sosyal medya, alışveriş siteleri, forumlar gibi üyelik isteyen uygulamalarda, Bakanlık tarafından verilen kurumsal e-Posta hesapları Bilgi Güvenliği Politikaları Kılavuzu kullanılamaz. Aksine durumlarda, yapılan tüm işlemlerden ve dile getirilen ifadelerden, ilgili kullanıcı sorumludur.

1.10.6. Konusu suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden ve sahip olduğu görev kapsamı içindeki iş ve işlemler dışındaki e-Posta hesabının kullanımından kullanıcı sorumludur.

1.10.7. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-Posta gönderilemez.

1.10.8. İnternet haber gruplarına üyelik için kurumun sağladığı e-Posta hesapları kullanılmaz. Ancak iş gereği üye olunması yararlı internet haber grupları için yöneticisinin onayı alınarak kurumun sağladığı resmi e-Posta adresi kullanılabilir.

1.10.9. Kullanıcılar, e-Posta hesaplarında hukuki açıdan suç teşkil edecek materyal ve belgeleri bulundurmaz. Kullanıcılar, kendi kullanıcı hesaplarında barındırdıkları içeriklerden ve gerçekleştirilen tüm elektronik posta işlemlerinden sorumludur.

1.10.10. Kurumsal e-Posta vasıtasıyla gizlilik dereceli veri aktarımı için Bilgi Güvenliği Politikaları Kılavuzu (e-Posta ile Veri Aktarımı) maddesinde belirtilen hususlara riayet edilir. e-Postaların, gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilir.

1.10.11. e-Posta gönderimlerinde, mesajın en alt kısmına gönderen kişinin kimlik ve iletişim bilgileri yazılır.

1.10.12. Kullanıcılar, gelen veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemek için her türlü tedbiri alır.

1.10.13. Tanınmayan elektronik postaların açılması, eklentilerinde bulunan dosya veya programların indirilip çalıştırılmasından kaynaklanabilecek güvenlik sorunlarının sorumluluğu kullanıcıya aittir.

1.10.14. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-Postalara yanıt verilmez.

1.10.15. Kaynağı bilinmeyen e-Posta ekinde gelen dosyalar kesinlikle açılmaz.

1.10.16. Kullanıcılar, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

1.10.17. e-Posta güvenliği ile ilgili şüpheli bir durum oluşması halinde ivedilikle sistem yöneticisine (eposta@saglik.gov.tr) haber verilir. Ayrıca <https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir> adresinde yer alan olay bildirim formu doldurulur.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ekrem MORAL Bilgi Güvenliği Yetkilisi	Erol ÖZTÜRK Personel ve Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Dr.Öğr.Üyesi Muhammet Ali ORUÇ İl Sağlık Müdürü



SAMSUN İL SAĞLIK MÜDÜRLÜĞÜ E-POSTA KULLANIMI VE PAROLA GÜVENLİĞİ KULLANIM POLİTİKASI



2. PAROLA GÜVENLİĞİ

- 2.1. Parola politikaları belirlenirken, sistem ve uygulamaların, kullanıcıları asgari olarak aşağıdaki kurallara uygun parola kullanmaya zorlamaları sağlanır.
- 2.2. Parolalar en az 8 (sekiz) karakterden oluşur. Root, administrator gibi sistem yönetim işlemlerinde kullanılan parolaların en az 12 karakterden oluşması tavsiye edilir.
- 2.3. İçerisinde en az 1 (bir) tane büyük ve en az 1(bir) tane küçük harf bulunur.
- 2.4. İçerisinde en az 1 (bir) tane rakam bulunur.
- 2.5. İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !,?,A,+,\$,#,&,/, {, *, ,,], =, ...)
- 2.6. Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, ababab...)
- 2.7. Sıralı karakterlerin kullanılması engellenir. (abcd, qwert, asdf,1234,zxcvb...)
- 2.8. Kişisel bilgiler veya klavye kombinasyonları ile basitçe üretilebilecek karakter dizilerinin kullanılması engellenir. (Örneğin 12345678, qwerty, doğum tarihi, çocuğun adı, soyadı gibi)
- 2.9. Sözlükte bulunabilen kelimelerin kullanılması engellenir.
- 2.10. Kullanıcının son 3 parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenir.
- 2.11. Sistem ve uygulamalarda oturum (session) kontrolü yapılarak bir kullanıcı adı ve parolasının aynı anda birden çok bilgisayarda kullanılması engellenir.
- 2.12. Veri tabanı yönetim sistemi, aktif izin sunucusu, uygulama sunucusu, ağ cihazları gibi sistem hesaplarına ait parolalar (root, administrator, vs.) en geç 3 (üç) ayda bir değiştirilir.
- 2.13. Kullanıcı hesaplarına ait parolalar (örnek: HBYS, e-posta, web, masaüstü bilgisayar vs.) en geç 6 (altı) ayda bir değiştirilmesi sağlanır.
- 2.14. Parolalar, e-posta iletilerine veya herhangi bir elektronik forma eklenmez.
- 2.15. Parolalar gizli bilgi olarak muhafaza edilir. Kişiyi özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.
- 2.16. Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da bu bölümde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.
- 2.17. İnternet tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup, kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.
- 2.18. Yazılım uygulamalarında erişim yetkisi tanımlanan kullanıcılara, gönderilen parola sıfırlama linkinin, aktivasyon işlemi başlatıldıktan (linke tıklandıktan) sonra en geç 15 dk. İçerisinde tamamlanacak şekilde konfigüre edilmesi gerekir.

YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla Bilgi Güvenliği Yönetim Sistemi Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ekrem MORAL Bilgi Güvenliği Yetkilisi	Erol ÖZTÜRK Personel ve Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Dr.Öğr.Üyesi Muhammet Ali ORUÇ İl Sağlık Müdürü