	T.C. SAĞLIK BAKANLIĞI ARDAHAN İL SAĞLIK MÜDÜRLÜĞÜ İnsan Kaynakları Ve Son Kullanıcı Güvenliği Prosedürü	

Kodu	Yayın Tarihi	Revizyon No	Revizyon Tarihi	Sayfa Sayısı / Num.
BY.PR.10	06.11.2018	1	03.07.2019	1/12

1. AMAÇ

Bu prosedürün amacı, T.C Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü ve Bağlı Birimler bünyesinde görev yapan/yapacak tüm personelin (kamu personeli, tam zamanlı ya da yarı zamanlı olarak çalışan sözleşmeli personel, yüklenici firma çalışanları, iş ortaklarının çalışanları, destek alınan firmaların personeli vb.) işe başlama, görev değişikliği ve işten ayrılma durumlarında izlenecek yöntemi tanımlamaktır.

2. KAPSAM

Bu prosedür, T.C Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü ve Bağlı Birimler bünyesinde görev yapan/yapacak tüm personeli (kamu personeli, tam zamanlı ya da yarı zamanlı olarak çalışan sözleşmeli personel, yüklenici firma çalışanları, iş ortaklarının çalışanları, destek alınan firmaların personeli vb.) kapsar.

3. TANIMLAR

İSM: Ardahan İl Sağlık Müdürlüğü
Bağlı Sağlık Tesisleri: Kamu Hastaneleri, Toplum Sağlığı Merkezleri, Entegre Hastaneler, Halk Sağlığı Laboratuvarı, İl Ambulans Servis Başhekimliği
KVKK: Kişisel Verileri Koruma Kurulu
VTYS: Veri Tabanı Yönetim Sistemi
SBA: Sağlık Bilgi Ağı
OGN: Ortak Giriş Noktası
ÇKYS: Çekirdek Kaynak Yönetim Sistemi
İKYS: İnsan Kaynakları Yönetim Sistemi
EBYS: Elektronik Belge Yönetim Sistemi
NES: Nitelikli Elektronik Sertifika
KPS: Kimlik Paylaşım Sistemi
MERNİS: Merkezî Nüfus İdare Sistemi
USS: Ulusal Sağlık Sistemi
KDS: Karar Destek Sistemi
HSYS: Halk Sağlığı Yönetim Sistemi
SBSGM: Sağlık Bilgi Sistemleri Genel Müdürlüğü
KamuSM: Kamu Sertifikasyon Merkezi

4. PROSEDÜR METNİ

4.1. İşe Alma Öncesinde Yapılacak Kontroller

4.1.1. Bilgi işleme tesislerine erişim izni verilecek tüm personel için (kamu personeli, tam zamanlı ya da yarı zamanlı olarak çalışan sözleşmeli personel, yüklenici firma çalışanları, iş ortaklarının çalışanları, destek alınan firmaların personeli vb.) işe alma öncesinde/alım yapılırken aşağıdaki hususların dikkate alınması gerekir.

4.1.2. İşe alma öncesinde yapılacak güvenlik kontrollerinin amacı, çalışanların kendilerinden beklenen sorumlulukları anlamalarını sağlamak ve düşünüldükleri roller için uygun olmalarını temin etmektir.

4.1.3. İşe alınacak adaylar iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilir (taranır).

4.1.4. Tarama yapılırken yürürlükteki yasal mevzuata mutlak şekilde uyulur. Yasal ve etik olmayan tarama yöntemleri kullanılmaz. Tarama esnasında oluşturulan/elde edilen kayıtlar uygun şekilde saklanır. Saklanmasına ihtiyaç duyulmayan kayıtlar bekletilmeksizin imha edilir.

4.1.5. İşe alınacak kişilerin eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilmesi için aşağıdaki yöntemlerden biri ya da birkaçı birlikte kullanılabilir

- Kişi özgeçmişinin doğrulanması (belgelerin tamlığı),
- Kişinin atanacağı görevle ilgili eğitim ve tecrübe açısından gerekli yeterliliğe sahip olmasının sağlanması,
- Beyan edilen akademik ve işle ilgili niteliklerin doğrulanması (diplomaların, referans mektuplarının, bonservis belgelerinin doğru ve geçerli olduğunun teyit edilmesi),
- 657 sayılı Kanun'un 48/8 maddesi gereği Yönetim Hizmetleri Genel Müdürlüğünce, devlet memurluğuna atanacak kişiler ile ilgili olarak 12 Nisan 2000 tarihli ve 24018 sayılı Resmi Gazetede yayımlanan "Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği" uyarınca "güvenlik soruşturması ve/veya arşiv araştırması" yaptırılması,
- 657 sayılı Kanun'a bağlı olmayan diğer personel için bağlı oldukları yasal mevzuatta yer alan hükümler uyarınca güvenlik incelemelerinin yaptırılması,
- Yüklenici personeli, destek personeli vb. statüde çalışacak personelin adli sicil kayıtlarının istenmesi ve incelenmesi.

4.1.6. Yükleniciler ile yapılan sözleşmelerde, idare tarafından yüklenici personeli için tarama yapılacağı ve tarama sonuçlarının menfi olması durumunda alınacak önlemler (örneğin personelin değiştirilmesi vb.) belirtilir.

4.1.7. İşe başlamadan önce tüm personel ve yükleniciler ile kişisel ve/veya kurumsal gizlilik sözleşmesi imzalanacağı ilgili taraflara bildirilir. İmzalatılacak sözleşmelerin içeriği ve ilgililerin yükümlülükleri detaylı olarak açıklanır. Sözleşmelerde kişilerin ve idarenin bilgi güvenliği sorumlulukları açıkça belirtilir.

4.1.8. Kuruluşun güvenlik ilkelerine uyulmaması durumunda, çalışanlar ve yükleniciler için yürütülecek işlemler (disiplin kurallarının uygulanması, gerekiyorsa iş akitlerinin sonlandırılması, tedarik sözleşmesinin feshi vb.) önceden belirlenir ve taraflara duyurulur

4.1.9. Personel birimi ilgili personelin gerekli bilgi ve belgelerini tamamladıktan sonra Personel İşe Başlama formunun kendi birimi ile ilgili bölümünü doldurur ve gerekli kayıt ve eğitimleri yapar.

4.1.10. Personel Personel İşe Başlama formunun diğer bölümleri için ilgili birimleri ziyaret eder, ilgili birimler kendileri ile formun ilgili bölümünü doldurur ve gerekli kayıt ve eğitimleri yapar.

4.1.11. Personel formlarda yazan bölümleri tamamladıktan sonra formu personel özlük birimine verir.

4.1.12. Personel birimi ilgili formu personelin özlük dosyasına koyar.

4.1.13. Bu süreç personelin işten ayrılmasın da veya görev değişikliğinde de aynı şekilde işletilir.

4.1.14. İşe başlayan her personele (kadrolu ve hizmet alımı dahil) bilgi güvenliği ve sosyal mühendislik zafiyetleri konularında eğitim verilir. Bu eğitimler uyum eğitimlerine dahil edilir.

4.1.15. Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.

4.1.16. Kullanacağı bilgi sistemlerine yönelik kullanıcı adı ve şifreleri tanımlanmalıdır. Şifreler her bölüm tarafından tanımlanır ve kapatılır.

4.1.17. İlgili personellere saglik.gov.tr uzantılı e-mail adresi alması sağlanmalıdır. İl içi yer değişikliklerinde ise sistem üzerinden kurum/birim değişikliği tanımlaması yapılmalıdır.

4.1.18. Tüm personele kurum kimlik kartı veya tanıtıcı yaka kimlik kartı personel birimi tarafından çıkartılır. Personel ayrılışında bu birim tarafından teslim alınır.

4.1.19. Kurumdan ayrılan personele ait "İşe Başlama Onay Formu" resmi yazı ile "Bilgi Güvenliği Yetkilisi/Temsilcisi" ne gönderilir.

4.1.20. Ayrılan personelin Kullandığı bilgi sistemlerine yönelik (TSİM, ÇKYS, EBYS, HBYS, MBYS, MKYS, SAĞLIK NET vb.) kullanıcı adı ve şifreleri sistem yöneticisi tarafından pasif hale getirilir.

4.1.21. İlgili formlar doldurulmadan personelin göreve başlayamaz ya da kurum ile ilişiği kesilmez.

4.2. İşe Alma Öncesinde Yapılacak Kontroller

4.2.1. Çalışma esnasında uygulanacak güvenlik kontrollerinin amacı, çalışanların işlerini yaparken bilgi güvenliği ile ilgili sorumluluklarının farkında olmalarını ve beklenen şekilde yerine getirmelerini sağlamaktır.

4.2.2. İşe yeni başlayan personelin başlayış işlemlerinin eksiksiz olarak yapılmasını sağlamak için "işe başlama formu" hazırlanır ve uygulanır.

4.2.3. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi sorumludur.

4.2.4. İşe başlama formunda bilgi güvenliği ile ilgili olarak personel giriş kartı çıkarılması ve bina/tesislere erişim için verilecek yetkiler, bilgi sistemlerine erişim için hesap açılması ve verilecek yetkiler (e-Posta, elektronik belge yönetim sistemi, hastane bilgi yönetim sistemi, insan kaynakları sistemi gibi), bilgi güvenliği farkındalık eğitimi, oryantasyon eğitimi, gizlilik sözleşmesi imzalatılması gibi hususlar mutlaka yer alır. (İşe başlama formu EK-01)

4.2.5. Üst yönetim, bilgi güvenliği politikalarını, prosedürlerini ve kontrollerini desteklediğini her fırsatta örnek teşkil edecek şekilde gösterir. Bu suretle, diğer çalışanların bilgi güvenliği ile ilgili

motivasyonları üst düzeyde tutulur.

4.2.6. Bilgi güvenliği ile ilgili beklentiler ve sorumluluklar, çalışanların görev tanımlarına eklenir.

4.2.7. Çalışanların kuruluşun bilgi güvenliği politikasına uyumu izlenir.

4.2.8. Tüm çalışanlar ve yükleniciler için bilgi güvenliği farkındalık eğitimi programları hazırlanır ve uygulanır.

4.2.9. Bilgi güvenliği ihlaline neden olan kişilere yapılacak işlemler (disiplin prosedürü) önceden belirlenir ve kişilere duyurulur. İhlal oluştuğunda, disiplin prosedüründe yazan hususlar uygulanır.

4.2.10. Bilgi güvenliği ihlali yapan personele uygulanan yaptırımlar (kişi kimlik bilgisi verilmeden) diğer çalışanlara duyurulur ve onlar için de örnek teşkil etmesi sağlanır.

4.3. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri

4.3.1. Kurumların bilgi güvenliği yetkililerince, bilgi güvenliği teknik ve farkındalık eğitimleri için yıllık olarak uygulanmak üzere bir eğitim planı hazırlanır.

4.3.2. Hazırlanan plan, kurumun bilgi güvenliği alt komisyonu tarafından onaylanır.

4.3.3. Teknik eğitimler için Sağlık Bakanlığı merkez teşkilatı, üniversitelerin sürekli eğitim merkezleri, diğer kamu kurum ve kuruluşları (TSE, TÜBİTAK vb.) ve konusunda uzmanlaşmış eğitim firmaları tarafından yapılan eğitimler tercih edilir. Eğitimler için ihtiyaç duyulan kaynak önceden planlanır ve ilgili yılın bütçesine yeterli ödenek koyulması sağlanır.

4.3.4. Bilgi işleme faaliyetlerinde kullanılan cihaz ve sistemlerin tedarik şartnamelerine, garanti süresini de içerecek şekilde, eğitim verilmesi ile ilgili hükümler konulur. Aynı şekilde cihaz ve sistemler için işletme, bakım, idame hizmet alımlarına, ihtiyaç varsa personelin eğitimine yönelik hükümler eklenir.

4.3.5. İşe yeni başlayan her personele, hassas bilgilere erişim izni verilmeden önce bilgi güvenliği farkındalığı eğitimi verilir. Farkındalık eğitiminde, genel bilgi güvenliği hususlarına ilave olarak anılan göreve yönelik özel bilgi güvenliği gereksinimleri de mutlaka yer alır.

4.3.6. Göreve başlama esnasında verilen eğitimlere ilave olarak her yıl tüm personele bilgi güvenliği farkındalık eğitimi verilir. Eğitimin mümkün ise sınıf ortamında veya seminer/konferans tarzında yüz yüze verilmesi tercih edilir. Personel sayısı ve coğrafi lokasyon farklılıkları nedeni ile eğitim yüz yüze yapılamıyorsa, uzaktan eğitim teknolojilerinden de istifade edilebilir. Eğitim uzaktan yapılacak ise asgari düzeyde de olsa etkileşim sağlanması (örneğin eğitimin başlangıcında ve sonrasında ön test ve son test yapılması gibi) gerekir. Farkındalık eğitimlerinin 32 Bilgi Güvenliği Politikaları Kılavuzu içeriğinin kişilere e-posta yoluyla iletilmesi veya web ortamında yayımlanan bir içeriğe kullanıcıların hiç bir etkileşim olmadan erişmelerinin sağlanması uygun yöntem olarak kabul edilmez.

4.3.7. Yüz yüze eğitimler haricinde özellikle bilgi teknolojilerinin sunmuş olduğu yetenekler/fırsatlar da kullanılmak suretiyle personelin farkındalık düzeylerinin artırılması sağlanır.

Bu kapsamda;

4.3.7.1. Bilgi güvenliği afişleri,

4.3.7.2. Bilgi güvenliği broşür ve el kitapları, e-bültenler,
4.3.7.3. Bilgisayarların açılış ekranlarına merkezi olarak konulacak ara yüzler,
4.3.7.4. İnternet tabanlı eğitim gibi araçlar kullanılabilir.

4.3.8. Sunulan bilgi güvenliği teknik ve farkındalık eğitimleri katılım öncesi ve sonrası çeşitli ölçme teknikleriyle ölçülür ve eğitim etkililiği hususunda değerlendirme yapılır.

4.3.9. Eğitim katılım formları hazırlanır, katılımcılara imzalatılır ve bilgi güvenliği alt komisyonu tarafından belirlenecek süre boyunca muhafaza edilir.

4.4. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri

4.4.1. Görev değişikliği veya işten ayrılma ile ilgili güvenlik kontrollerinin amacı, ayrılma işlemleri esnasında yapılması gereken bilgi güvenliği ile ilgili tedbirlerin ortaya konulması ve çalışanların görevleri sona erse dahi bilgi güvenliği ile ilgili devam eden sorumlulukları hakkında bilgilendirilmesidir.

4.4.2. Kişi, görevi esnasında edinmiş olduğu bilgileri, görev yeri değişmesi veya ayrılması durumunda dahi sır olarak saklamaktan ve hiçbir şekilde yetkisiz olarak ifşa etmemekten sorumludur. Sır saklama yükümlülüğü süresizdir.

4.4.3. İşten ayrılan veya görev değişikliği yapan personelin ayrılma işlemlerinin bilgi güvenliği açısından eksiksiz olarak yapılmasını sağlamak için "işten ayrılma formu" hazırlanır ve uygulanır. (İşten ayrılma formu EK-02)

4.4.4. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi ile insan kaynakları birimi müştereken sorumludur.

4.4.5. İşten ayrılan veya görev yeri değişen kişinin eski görevi ile ilgili bilgisayar hesapları ve uzaktan erişim için kullandıkları hesaplar kapatılır veya erişim yetkileri yeni görev yerinin gereksinimlerine göre yeniden düzenlenir.

4.4.6. Kişiye teslim edilmiş tüm bilgi varlıkları (bilgisayarlar, yazılı ortamda saklanan bilgi ve belgeler, bilgisayar ortamında tutulan dosyalar, lisans belgeleri, CD'ler vb.) sayım yapılarak iade alınır.

4.4.7. Ayrılan veya görev yeri değişen personel tarafından yürütülen faaliyetlerin aksamaması için birim sorumlusu tarafından gerekli tedbirler alınır.

4.4.8. Mümkünse ayrılan personel ile yeni katılan personelin geçici bir süre birlikte görev yapması sağlanır.

4.4.9. Ayrılan kişiden teslim alınan bilgisayarlar güvenli silme işlemi yapılmadan bir başka kullanıcıya teslim edilemez.

4.5. Kullanıcıların Bilgi Güvenliği Sorumlulukları

4.5.1. Personel, T.C. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzu'nda yer alan koşullara uygun hareket eder. Burada yer alan hükümleri kişisel olarak ihlal etmesi halinde Bakanlığa, görev yaptığı kuruma ve üçüncü kişilere vereceği her türlü zarardan sorumludur.

4.5.2. Personel, görev yaptığı kurum tarafından kendisine teslim edilmiş veya erişim yetkisi verilmiş olan bilgileri, sadece görevi ile ilgili işler için kullanır. Bu bilgileri kendi gizli bilgisi gibi korur ve bilmesi gereken yetkili kişiler haricinde hiçbir kimse ile paylaşmaz. Personel, bilgi paylaşabileceği kişiler konusunda şüpheye düşerse, bilginin sahibi olan veya süreci yöneten birim ile irtibata geçerek veriyi kimlerle paylaşabileceğini teyit eder.

4.5.3. Personel, özel olarak yetkilendirildiği durumlar dışında, hizmet verilen tarafların yetkilileri de dâhil olmak üzere yetkisi olmayan hiçbir kişi ile bilgi paylaşımı yapmaz. Yetkisi olmadığı halde bulunduğu görev ve makamı kullanarak kendisinden ısrarla bilgi talep eden kişileri en yakın amirine bildirir.

4.5.4. Personel, görevi kapsamında kendisine teslim edilmiş olan bilgileri ilgili mevzuata uygun olarak korur, işler ve aktarır. Görev yaptığı kuruma ait bilgileri, yetkisi olmayan üçüncü kişilerin yanında konuşmaz.

4.5.5. Personel, edindiği bilgileri hiçbir kişi, grup, kurum veya kuruluşun menfaati için kullanamaz.

4.5.6. Bakanlığımızda kullanılan bilgi sınıflandırması ile ilgili hususlar Kılavuz'un 4.3 (Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi) numaralı maddesinde açıklanmıştır. Bu kapsamda usulüne uygun olarak sınıflandırılmamış ve etiketlenmemiş olsa dahi; Bakanlığa veya hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgisayar ve telekomünikasyon sistemleri içerisinde saklanan veriler, donanım-yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduğu tüm işler gizlidir. Bunların, görevin gerektirdiği durumlar haricinde kullanılması kesinlikle yasaktır.

4.5.7. Personel, görevi ile ilgili olsun veya olmasın edindiği ve gizlilik arz eden her türlü bilgiyi sır olarak saklamak ve bunları üçüncü kişilere hiçbir şekilde iletmemekle yükümlüdür.

4.5.8. Bu yükümlülük, personelin görev yaptığı kurum ile ilişkisinin sona ermesi halinde de devam eder.

4.5.9. Personel, görevi nedeniyle edindiği gizli bilgiler hakkında, hiçbir sebeple yazılı veya sözlü açıklama yapamaz.

4.5.10. Personel, görevi kapsamında erişim hakkının bulunduğu sistemleri ve bilgileri, yetkisi içinde ya da yetkisini aşarak kendisine veya bir başkasına çıkar sağlamak amacıyla kullanamaz.

4.5.11. Personel, bilgi sistemlerinde kullanılan/yer alan programları, verileri veya diğer unsurları hukuka aykırı olarak ele geçirme, değiştirme, silme girişiminde bulunamaz ve bunları nakledemez veya çoğaltamaz.

4.5.12. Personel, başkasına zarar vermek ya da kendisine veya başkasına haksız yarar sağlamak maksadıyla yahut herhangi bir maksat gütmeksizin, kullandığı bilgi işleme ortamlarını ve bu ortamlarda saklanan verileri kısmen veya tamamen tahrip etmek, değiştirmek, silmek, sistemin işlemesine engel olmak veya yanlış biçimde işlemesini sağlamak gibi davranışlarda bulunamaz.

4.5.13. Personel, hangi amaçla olursa olsun görevi kapsamında edindiği bilgileri, bilgi işleme ortamlarında çeşitli şekillerde (basılı, manyetik vb.) bulunabilecek olan verileri, yetkisiz ve izinsiz olarak kullanamaz, kopyalayamaz, taşıyamaz ve aktaramaz.

4.5.14. Personel, görev yaptığı kurum tarafından kendisine verilen ya da tanımlanan kullanıcı adını/parolayı hiç kimseyle paylaşmaz. Parolasının gizli kalması için alınması gereken tüm tedbirleri alır. Kurumdan ayrılması halinde Bilgi Güvenliği Politikaları Kılavuzu 35 kullanıcı

adını/parolayı iptal ettirir. Kullandığı bilgisayar ve/veya diğer elektronik veri depolama cihazlarında oluşturduğu veri, bilgi ve belgeler dâhil tüm belgeleri, cihazları ve ofis malzemelerini eksiksiz olarak ilgilisine teslim eder ve bunların hiçbir kopyasını alamaz.

4.5.15. Personel, görev yaptığı kuruma ait sunucular üzerinden kendisine tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP adresini kullanarak gerçekleştirdiği her türlü etkinlikten, Kurum bilişim kaynakları kullanılarak oluşturduğu ve/veya kendisine tahsis edilen Kurum bilişim kaynağı üzerinde bulundurduğu her türlü içerikten (kayıt, doküman, yazılım vb.) sorumludur.

4.5.16. Personel, 5651 sayılı Kanun gereği tutulması gereken kayıtlara ilave olarak; Bakanlık ve görev yaptığı kurum tarafından uygun görülen diğer sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının iz kayıtlarının hukuki süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla toplanabileceğini kabul eder.

4.5.17. Kişinin kendi kusuru nedeniyle parolasının ifşa olması durumunda, başkası tarafından yapılmış olsa dahi personele teslim edilen kullanıcı adı ve parolalar ile yapılan iş ve işlemlerden ilgili personel şahsen sorumludur.

4.6. Elektronik Posta Güvenliği

4.6.1. Bakanlığımızda görev yapan personel tarafından görevleri gereği yürütülen kurumsal iş ve işlemlerde, *@saglik.gov.tr uzantılı kurumsal veya tüzel e-Posta hesabı kullanılır. Kurumsal iş ve işlemler, kişilerin özel işleri için (Gmail, Hotmail gibi) internet hizmet sağlayıcılarından alınan hesaplar üzerinden yürütülmez.

4.6.2. KVKK tarafından 6698 sayılı Kanun'da 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 yasal zorunluluktur.

4.6.3. Bakanlığımızda görev yapan tüm kamu personeline, talep etmeleri halinde kurumsal e-Posta hesabı açılır.

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

4.6.5. Kurumsal e-Posta adresi isimlendirme politikası, istisnai durumlar dışında "ad.soyad@saglik.gov.tr" şeklindedir. Yeni bir kullanıcı oluşturulurken o kullanıcının adı ve soyadı ile daha önce bir hesap açılmış ise "ad.soyad" kombinasyonunun ardına her seferinde bir artacak şekilde sıradaki sayı eklenir. (akin.koc2, akin.koc3 gibi).

4.6.6. 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 işlev ile alakalı olarak belirlenir. (bilgiguvenligi@saglik.gov.tr, some@saglik.gov.tr gibi).

4.6.7. Kurumsal ve tüzel e-Posta hesabı açılması için başvuru usulleri ve ilgililerince yapılacak işlemler Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuz'nun 6.5 (Merkezi Aktif Dizin ve E-Posta Sistemine Erişim) maddesinde belirtildiği gibi yapılacaktır.

Merkezi Aktif Dizin ve E-Posta Sistemine Erişim

- SBSGM tarafından Bakanlık merkez teşkilatı birimlerinin etki alanı hizmetlerinin gerçekleştirilmesi, tüm Bakanlık kullanıcılarına *@saglik.gov.tr uzantılı e-Posta hesaplarının açılması maksadıyla "Merkezi Aktif Dizin ve e-Posta Sistemi" kurulur ve işletilir.
- Aktif dizinde kurumsal birim (Organizational Unit: OU) yaratma, silme, değiştirme; OU'lar altında yeni kullanıcı tanımlama, kullanıcı hesabını askıya alma (disable), silme, kullanıcı özelliklerini değiştirme, kullanıcıyı teşkilat ağacında bir noktadan diğer noktaya taşıma; kullanıcı için e-Posta hesabı açma, e-Posta hesabını askıya alma, e-Posta hesabını silme gibi işlemler SBSGM tarafından (Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı) yapılır.
- Merkezi aktif dizin hizmetinin e-Posta işlemleri dışında başka maksatlarla kullanılması gerektiğinde (örneğin geliştirilen bir uygulama için kullanıcı erişim yetkilendirmesi) yazılı talepte bulunulur. Bu tür erişim taleplerinde prensip olarak sadece "okuma yetkisi" ile erişim izni verilir. Farklı yetkiler ile aktif dizin erişim taleplerine, SBSGM BGYS politikaları kapsamında yapılacak risk değerlendirmesinde alınacak karara istinaden işlem yapılır.

Gerçek kişiler için kurumsal e-Posta hesap işlemleri:

- Bakanlık merkez ve taşra teşkilatı ve bağlı kurumlarda görev yapan gerçek kişiler, ÇKYS/İKYS sisteminde kayıtlı iseler, kişisel olarak https://eposta.saglik. gov.tr/ adresindeki "Kayıt Ol" menüsündeki adımları takip etmek suretiyle "*@ saglik.gov.tr uzantılı" "kurumsal e-Posta hesabı" açarlar.
- ÇKYS/İKYS sisteminde kayıtlı olmayan personel için "KLVZ-EK-08 e-Posta Talep Formu / Gerçek Kişiler" ilgili birimler tarafından doldurularak üst yazı ile SBSGM'ye gönderilir.
- SBSGM tarafından formda isimleri yazan personelin ÇKYS/İKYS kayıtlarında olup olmadığı ve hâlihazırda anılan kişi adına açılmış bir e-Posta hesabı bulunup bulunmadığı kontrol edilir.
- Talep edilen "kurumsal e-Posta hesapları" açılır. Hesaplara ait tek kullanımlık erişim şifreleri kapalı zarf içinde resmi yazı ile talep yapılan birimlere iletilir.
- Tek kullanımlık şifrelerin, gizliliği bozulmadan hesap açılan gerçek kişilere ulaştırılması, resmi yazıya işlem yapan birimin sorumluluğundadır.

Ortak kullanım için tüzel e-Posta hesap işlemleri:

- Tüzel e-Posta hesapları birden fazla gerçek kişi tarafından erişilebilen ve belli bir görevin icrası veya bir birim adına yürütülen faaliyetlerin gerçekleştirilmesi (satınalma@saglik.gov.tr, ik@saglik.gov.tr, bilgiguvenligi@saglik.gov.tr gibi) için açılır.
- Tüzel e-Posta hesaplarına kimin hangi yetki ile erişeceği "KLVZ-EK-09 E-Posta Talep Formu/Tüzel Kişiler" doldurulmak suretiyle, üst yazı ile SBSGM'ye gönderilir.
- Tüzel e-Posta hesabının açılmasını müteakip yetki verilen kişiler, ortak posta kutusunu, kişisel olarak kullandıkları kurumsal e-Posta kutuları altında ikinci bir posta kutusu olarak görmeye ve kullanmaya başlarlar.
- Ortak posta kutusuna erişecek kişiler ve erişim yetkisi değişiklik talepleri, ortak posta

kutusundan epostayonetim@saglik.gov.tr adresine bildirilmesi suretiyle yapılır.

- Kullanıcı hesaplarının ve posta kutularının yönetimi
- Sistem yönetim araçları ile aktif dizin kullanıcı hesapları taranarak bir yıldan daha uzun süredir kullanılmayan kullanıcı hesapları pasife alınarak kullanıma kapatılır.
- Kurumdan ayrılan, emekli olan, ilişiği kesilen personelin kullanıcı hesapları pasife alınarak kullanıma kapatılır.

4.6.8. 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.

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

- Kullanıcıların e-Posta hesaplarına tarayıcı programları, masaüstü istemci uygulaması (Office Outlook) ve cep telefonları üzerinden güvenli olarak erişebilmeleri için gerekli servisler sağlanır.
- 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.
- Kullanıcı parolalarının Kılavuz'un 6.3 (Parola Güvenliği) maddesinde belirtilen politikalar ile uyumlu olup olmadığı denetlenir.
- Bakanlık e-Posta sistemi tarafından oluşturulan ve sisteme ilk kez girişte kullanılan parolanın ilk kullanımdan sonra değiştirilmesi sağlanır.
- Kullanıcıların son kullandığı üç parolayı kullanması engellenir.
- Kullanıcılar, altı ayda bir parolalarını değiştirmeye zorlanır. Parola değiştirme süresine beş (5) gün kala uyarı iletisi gönderilir.
- 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.
- 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.
- Bir yıl süre ile sisteme giriş yapmayan kullanıcıların hesapları geçici olarak kapatılır. Bu hesaplar aktif dizinde pasife çekilir.
- 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.

- 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.
- Yüksek sayıda üye içeren dağıtım grupları, tüm kullanıcılar tarafından görülen genel adres defterinden gizlenir.
- Bir e-Postaya eklenebilecek en fazla alıcı sayısı 100 (yüz) e-Posta adresi ile sınırlı tutulur.
- Gönderilen e-Posta boyutu 25 MB'yi geçemez.
- Dağıtım gruplarının kullanım durumları (e-Posta akış trafiği) takip edilir ve bir yıl boyunca kullanılmayan gruplar tespit edilerek silinir.
- E-Posta iletimlerinde "exe" gibi çalıştırılabilir dosyaların gönderilmesi engellenir.
- E-Posta sistemlerinde fazla veri (data) boyutu oluşturması sebebi ile e-Posta hesaplarına profil resmi eklenmesi engellenir.
- *@saglik.gov.tr uzantılı e-Posta hesabından farklı uzantılı e-Posta adreslerine gönderilen iletilerde e-Posta Yasal Uyarı (Disclaimer) metni gönderilir.
  Bilgi Güvenliği Politikaları Kılavuzu Yasal Uyarı: Bu e-Postanın içerdiği bilgiler (ekleri de dâhil olmak üzere) gizlidir. T.C. Sağlık Bakanlığı onayı olmadan içeriği kopyalanamaz, üçüncü kişilere açıklanamaz veya iletilemez. Bu mesajın gönderilmek istendiği kişi değilseniz ya da bu e-Postayı yanlışlıkla aldıysanız, lütfen yollayan kişiyi haberdar ediniz ve mesajı sisteminizden derhal siliniz. T.C. Sağlık Bakanlığı bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda bir garanti vermemektedir. Bu nedenle, bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından ve saklanmasından T.C. Sağlık Bakanlığı sorumlu değildir. Bu mesajın içeriği yazarına ait olup, T.C. Sağlık Bakanlığı görüşlerini içermeyebilir. Bu e-Posta bizce bilinen tüm bilgisayar virüslerine karşı taranmıştır.

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

- Kullanıcılar, kendilerine tahsis edilen e-Posta hesabını bir başka kişiye kullandıramaz veya devredemez.
- Kullanıcılar, parolalarını Kılavuz'un 6.3 (Parola Güvenliği) maddesinde belirtilen parola politikaları uyarınca oluşturur ve kullanır.
- Kullanıcılar, kendilerine ait parolanın güvenliğinden ve söz konusu parola kullanılarak gönderilen e-Postalardan doğacak hukuki işlemlerden sorumludur.
- 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 kullanıcısına aittir.
- Sosyal medya, alışveriş siteleri, forumlar gibi üyelik isteyen uygulamalarda, Bakanlık tarafından verilen kurumsal e-Posta hesapları Bilgi Güvenliği Politikaları Kılavuzu 39 kullanılamaz. Aksine durumlarda, yapılan tüm işlemlerden ve dile getirilen ifadelerden, ilgili kullanıcı sorumludur.

- 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.
- Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-Posta gönderilemez.
- 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.
- Kullanıcılar, e-Posta hesaplarında hukuki açıdan suç teşkil edecek materyal ve belgeleri bulunduramaz. Kullanıcılar, kendi kullanıcı hesaplarında barındırdıkları içeriklerden ve gerçekleştirilen tüm elektronik posta işlemlerinden sorumludur.
- Kurumsal e-Posta vasıtasıyla gizlilik dereceli veri aktarımı için Kılavuz'un 10.4.17 (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.
- E-Posta gönderimlerinde, mesajın en alt kısmına gönderen kişinin kimlik ve iletişim bilgileri yazılır.
- Kullanıcılar, gelen veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemek için her türlü tedbiri alır.
- Tanınmayan elektronik postaların açılması, eklentilerinde bulunan dosya veya programların indirilip çalıştırılmasından kaynaklanabilecek güvenlik sorunlarının sorumluluğu kullanıcıya aittir.
- Spam, zincir, sahte vb. zararlı olduğu düşünülen e-Postalara yanıt verilmez.
- Kaynağı bilinmeyen e-Posta ekinde gelen dosyalar kesinlikle açılmaz.
- Kullanıcılar, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.
- 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.

4.7. Sosyal Mühendislik ve Sosyal Medya Güvenliği

4.7.1. Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanır. Başka bir tanım ise insanoğlunun zaaflarını kullanarak istenilen bilgiyi, veriyi elde etme sanatıdır.

4.7.2. Sosyal mühendislik yapan kötü niyetli kişiler, sosyal medya ve analiz yöntemlerini kullanarak hedef kişiler hakkında bilgi toplarlar. Sonrasında sosyal mühendislik tekniklerini kullanarak insanların zaaflarından faydalanıp istedikleri bilgilere ulaşmak için çalışma yaparlar.

4.7.3. Sosyal mühendislik saldırılarından korunmak için kişisel olarak dikkat edilmesi gereken hususlar şu şekildedir:

- Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunuz.
- Bilgilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket ediniz.
- Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat ediniz.
- Özellikle telefonda, e-Posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgilerinizi kesinlikle paylaşmayınız
- Parola kişiye özel bilgidir. Sistem yöneticiniz dâhil telefonda veya e-Posta ile parolanızı hiç kimseyle kesinlikle paylaşmayınız.
- Oluşturulan dosyaya erişecek kişiler ve haklarını, "bilmesi gereken" prensibine göre belirleyiniz ve erişim kontrol tedbirleri uygulayınız.
- Verdiğiniz erişim haklarını belirli dönemlerde kontrol ediniz.
- Çöpe atılan kâğıtlara dikkat ediniz. Kişisel veri içeren ya da kuruma ait bilgilerin yer aldığı kâğıtları, kâğıt kırpma makinesinde imha ediniz.
- Çok acele bilgi istendiği zaman istenen bilginin niteliğine göre teyit mekanizması kullanınız.
- Bilgisayarınızı yabancı bir kişiye kullandırmayınız. Bu kişiler tarafından bilgisayarınıza takılacak olan USB depolama aygıtları ya da harici disklerden bilgisayarınıza zararlı yazılım bulaştırabilir.
- Hediye olarak verilen USB depolama aygıtlarını kullanmadan önce mutlaka virüs taramasından geçiriniz.

4.7.4. Hastanelerde sosyal mühendislik alanında alınacak bazı önlemler şu şekilde sıralanabilir:

- Kişisel sağlık kayıtlarının (tüm tetkik sonuçları, hasta dosyaları, barkodlar, gözlem formları vb.) özel nitelikli kişisel veri kategorisinde olduğu ve 6698 sayılı Kanun ile özel koruma uygulanması gerektiği her zaman dikkate alınır.
- Telefon ile hasta hakkında bilgi almak isteyen kişilere, hastanın kişisel bilgileri ile ilgili açıklama yapılmaz. 3
- Hasta dosyaları, hastanın tedavi sürecine dâhil olan sağlık profesyonelleri/ çalışanları dışında kimseyle paylaşılmaz. Kolay ulaşılır yerlere konulmaz.
- Sağlık Bilgi Yönetim Sistemi (SBYS) programlarında kullanılan parolalar kimseyle paylaşılmaz.

4.7.5. Kişisel Sosyal Medya Güvenliği

- Sosyal medya hesaplarına giriş için kullanılan parolalar ile kurum içinde kullanılan parolalar farklı seçilir.
- Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.
- Kuruma ait gizli bilgiler, resmi yazılar, çeşitli gelişmeler sosyal medya ortamında yayımlanamaz.

  Eğitimlerde sosyal medya güvenliği ile ilgili hususlara yer verilir.

T.C.
SAĞLIK BAKANLIĞI
ARDAHAN İL SAĞLIK MÜDÜRLÜĞÜ
İnsan Kaynakları Ve Son Kullanıcı Güvenliği
Prosedürü

Hazırlayan	Kontrol Eden	Onaylayan
Oğuz KARABAĞ Bilgi Güvenliği Yetkilisi	Uz. Dr. Nejat AKIN Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Op. Dr. Erkan ÖZDEMİR İl Sağlık Müdürü