T.C. SAĞLIK BAKANLIĞI
Kamu Hastaneleri Genel Müdürlüğü

VERİMLİLİK VE KALİTE UYGULAMALARI DAİRE BAŞKANLIĞI

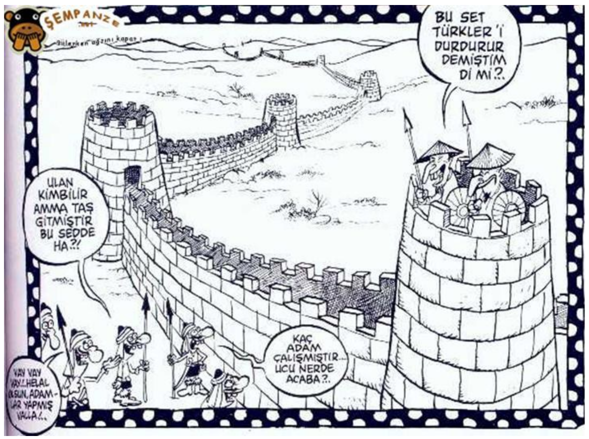
KAMU HASTANELERİ GENEL MÜDÜRLÜĞÜ

VERİMLİLİK VE KALİTE UYGULAMALARI DAİRE BAŞKANLIĞI

BİLGİ YÖNETİM SİSTEMİ

Dilek KARAKAYA
Sağlık Bilgi Sistemleri Genel Müdürlüğü
Bilgi Güvenliği Yönetim Sistemleri Birim Sorumlusu
dilek.karakaya@saglik.gov.tr

NİSAN 2018


ŞEMPANZE
Gülerken ağzını kapat!
BU SET TÜRKLER'İ DURDURUR DEMİŞTİM Dİ Mİ?.
ULAN KİMBİLİR AMMA TAŞ GİTMİŞTİR BU SEDDE HA?!
KAÇ ADAM ÇALIŞMIŞTIR UCU NERDE ACABA?.
VAY VAY VAY!..HELAL OLSUN, ADAMLAR YAPMIŞ VALLA!..

- Güvenliğin sadece % 20 lik kısmı teknik güvenlik önlemleri ile sağlanıyor.
- % 80 i ise son kullanıcıya bağlı.

http://ab.org.tr/ab09/kitap/sahinaslan_kanturk_AB09.pdf

Bilgi Güvenliği Kavramı

Teknolojinin Hayatımıza Etkileri


İNSANIN TEMEL İHTİYAÇLARI
kendini gerçekleştirme
değer ihtiyaçları
ait olma ve sevgi ihtiyacı
güvenlik ihtiyacı
fizyolojik ihtiyaçlar
WiFi

Bilgi Nedir?

Bilgi, kurumun ve kişinin en değerli varlığıdır. Korunması ve verimli kullanılması sağlanı

Bulunduğu yerler;

- İnsanda (Sözlü)
- Kağıt üzerinde
- Bilgisayar sistemlerinde
- Fiziksel ortamlarda -...

Bilgi Güvenliği Yönetim Sistemi (BGYS):

Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere; sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, kurumun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününü,

21.06.2017 Kamu Net Tebliği

Bilgi Güvenliği Nedir?

- **Gizlilik**; Bilginin yetkisiz kişiler, varlıklar ya da süreçlere kullanılabilir yapılmama ya da açıklanmama özelliğini,
- **Bütünlük**; Varlıkların doğruluğunu ve tamlığını koruma özelliğini,
- **Erişilebilirlik**; Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğini,

Bilgi Güvenliği Neden Önemlidir?

BİLGİ GÜVENLİĞİ ZAFİYETLERİ NELERE YOL AÇAR?

- Bir hastanenin hastaları ile ilgili kişisel bilgileri ele geçirilebilir.
- Sosyal medyada kurum itibarına zarar verecek bilgiler yayınlanabilir.
- Sağlık çalışanlarının parolaları ele geçirilerek yasa dışı işler yapılabilir.
- Kurum çalışanlarına ait kişisel bilgiler, internet ortamından denetimsiz olarak erişilebilir.
- İnteraktif bankacılık sistemi ile kullanıcıların hesaplarındaki paralar çalınabilir.
- Öğrencilerin notları, okul kayıtları yetkisiz olarak değiştirilebilir.
- İnternet kullanıcılarının bilgisayarları ele geçirilerek, kullanıcı farkına bile varmadan bilgisayar üzerinden kurumsal sistemlere saldırılabilir.
- Ele geçirilen bilgisayarlar aracılığıyla topluca istenmeyen e-postalar gönderilebilir.

- CAN KAYIPLARI OLABİLİR!!!!!

Bilgi Güvenliği Nedir?

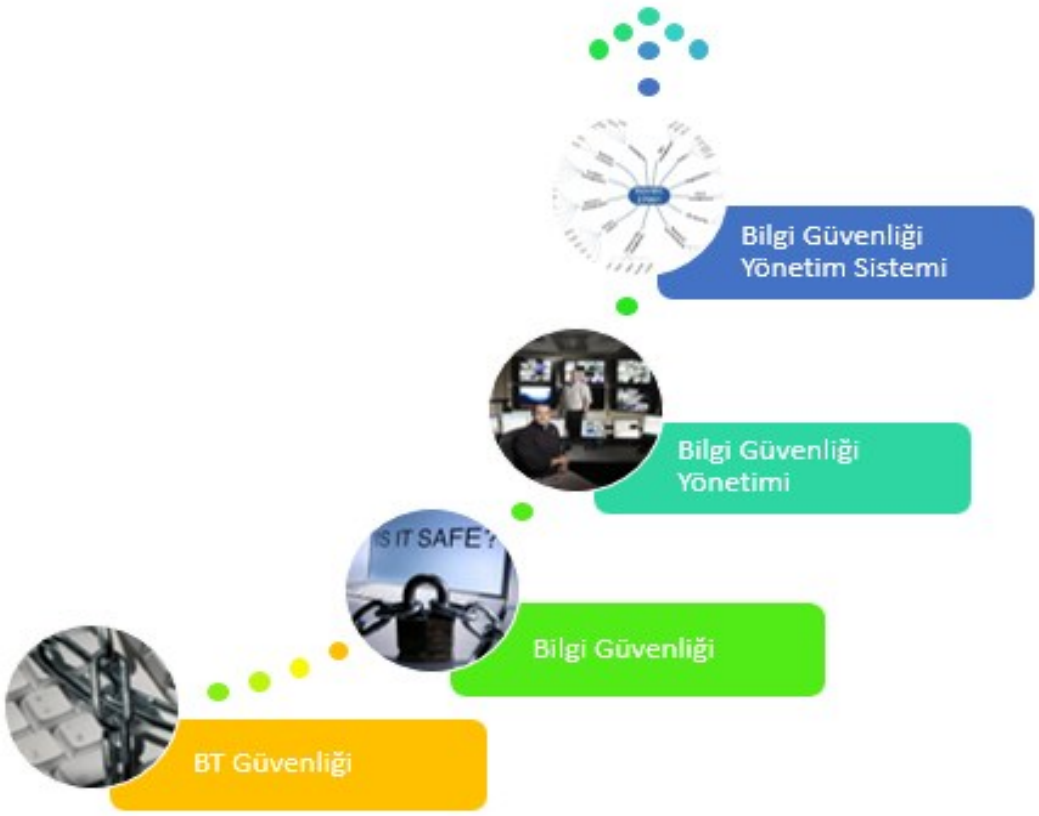
Politikalar, Prosedürler, Standartlar ve Süreçler
(Bilgi Güvenliği Politikası, Bilgi Varlıklarının Yönetimi, Yedekleme Prosedürü vb.)

Üç Önlemde Birlikte Yürütülmedikçe Bilgi Güvenliğinden Söz Edilemez...

İş Sözleşmesi
Bilgi Güvenliği El Kitabı
Oryantasyon Eğitimleri
Duyuru ve Bilgilendirme Çalışmaları

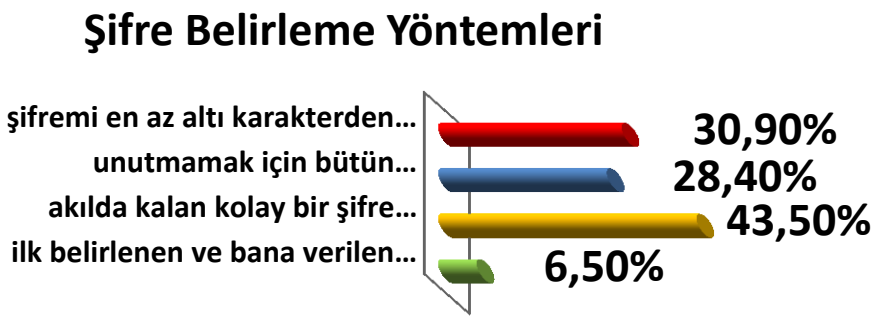
Güvenlik Duvarı
Antivirüs Yazılımı
Loglama Çözümleri
Kullanıcı Adı ve Parola Kullanımı

Bilgi Güvenliği Nedir?

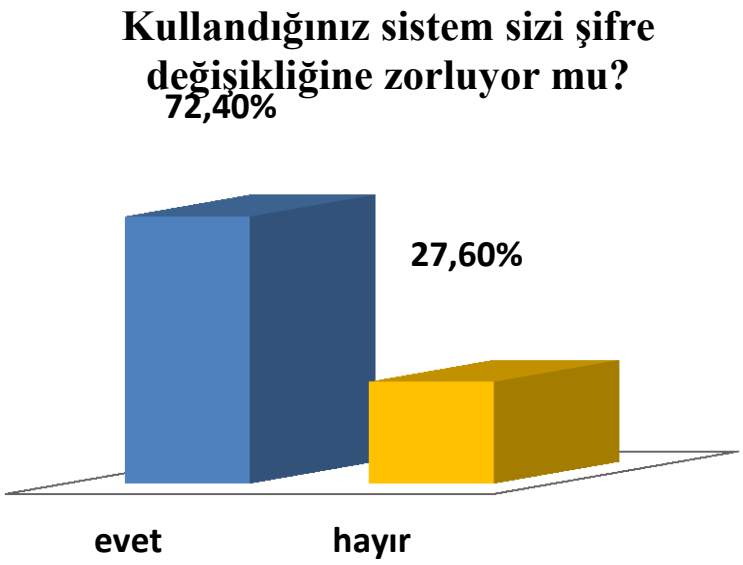


‘Güvenlik bir ürün değil, bir süreçtir.’ Bruce SCHNEIR

Bilgi Güvenliği Farkındalığı Anket Sonucu



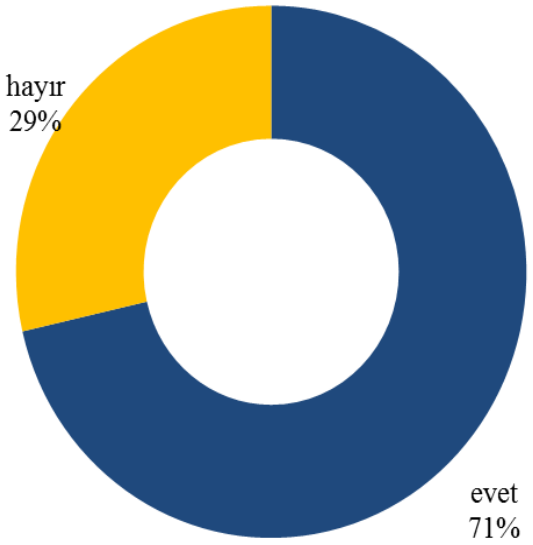
Bilgi Güvenliği Farkındalığı Anket Sonucu



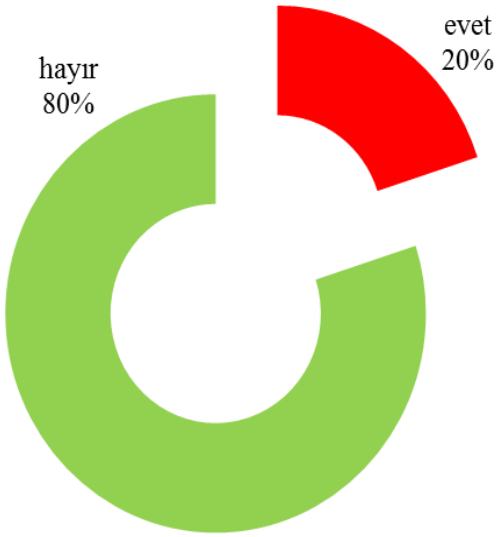
MADDE 136. - (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Bilgi Güvenliği Farkındalığı Anket Sonucu

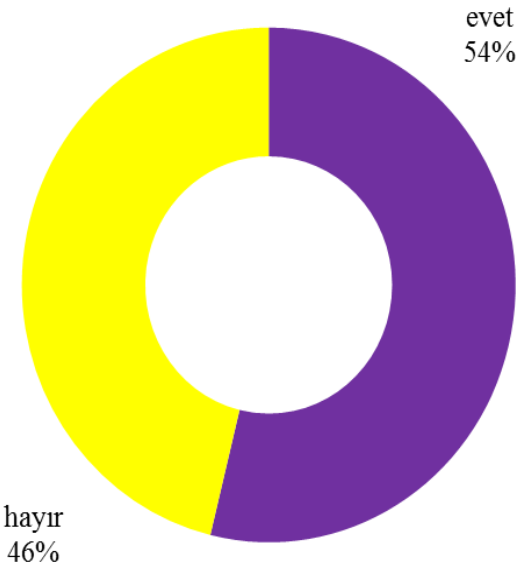
Doktorlar şifrelerini sizinle paylaşır mı?



Hastaların kişisel bilgilerini başka şahıslarla paylaşır mısınız?



Hemşireler şifrelerini sizinle paylaşır mı?



Doktorların parolası çalındı binlerce ilaç yazıldı

Sağlık sektörünü gözüne kestiren dolandırıcılık şebekeleri, doktorların e-reçete şifrelerini çaldı. Şebeke, yüksek tutarlı ilaçları hastalar üzerine yazmaya başladı. Vatandaşlar ilaç katkı payı Ödemek zorunda kaldı.

ELEKTRONİK İMZA = ISLAK İMZA

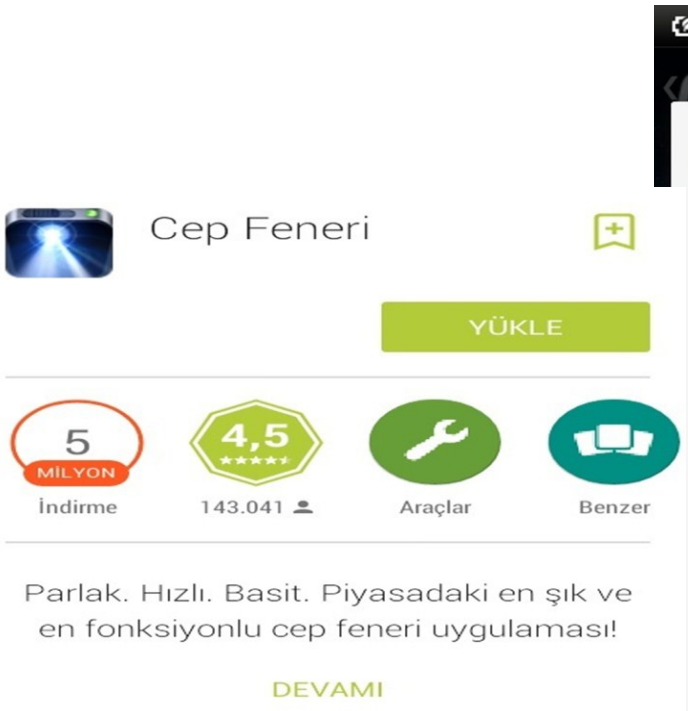
00.02/698 sayılı yazısı
2-Hukuk İşleri Genel Müdürlüğünün 21.05.2007 tarih ve B.03.O.HİG.0.00.00.03
-647.03.01-46-2007 / 1214 sayılı yazısı

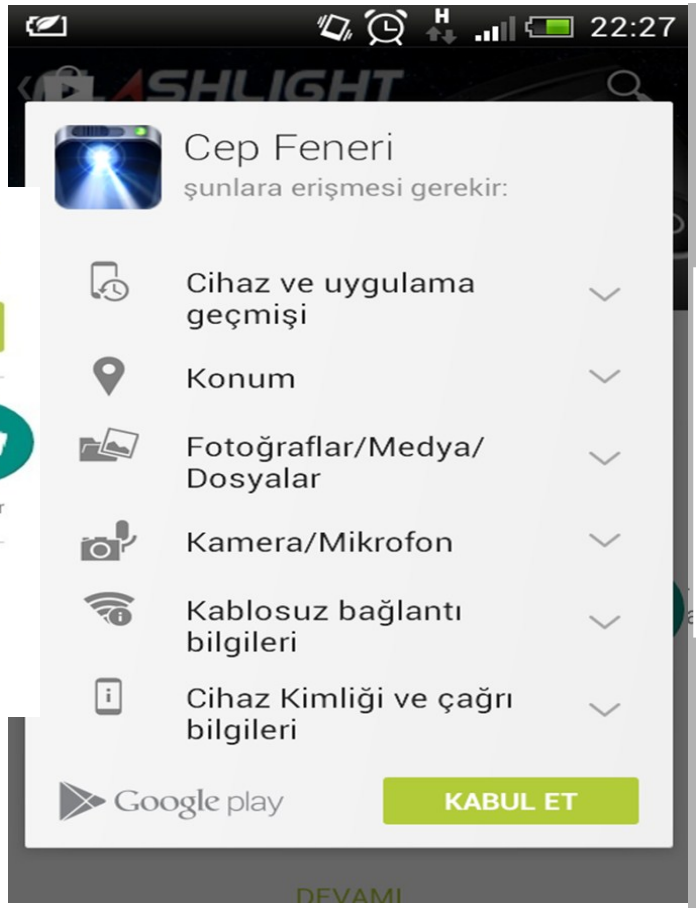
Elektronik İmza Kanunu'nun 4 üncü maddesine göre güvenli elektronik imza; "münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan ve imzalanmış elektronik veride, sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan" imza türüdür.

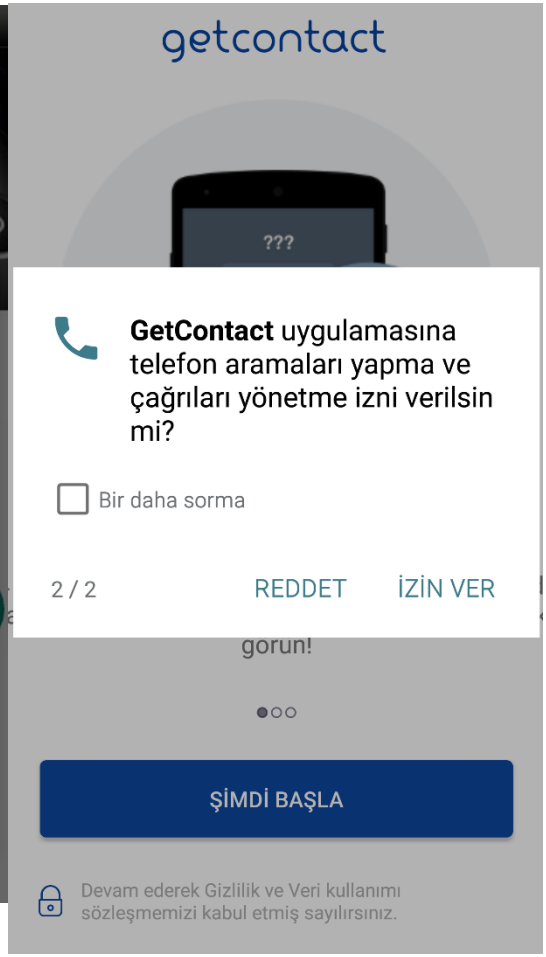
Güvenli elektronik imza, bir kişi tarafından gönderilen bilgilerin veya verilerin kesinlikle o kişi tarafından gönderildiğini teyit, başkası tarafından gönderilmediğini garanti eder. Dolayısıyla, klasik imzadaki gibi taklit edilme olasılığı da ortadan kalkar. Gönderici göndermediğini, alıcı da almadığını iddia edemez.

5070 sayılı Elektronik İmza Kanunun 5 inci, 1086 sayılı Hukuk Usulü Muhakemeleri Kanununun 295/a ve 818 sayılı Borçlar Kanununun 14 üncü maddeleri uyarınca ***güvenli elektronik imza*** el ürünü imza (ıslak imza) ile aynı hukuki değere sahip bulunmakta ve aynı işlevleri yerine getirmektedir.

Akıllı Telefonlar







GD.13.1. Bilgi güvenliğinden sorumlu bir ekip oluşturulmalıdır.

Sağlık tesisinde bilgi güvenliğini sağlamak amacıyla bir ekip oluşturulmalıdır. Bu ekip, üst yönetiminden bir yöneticinin başkanlığında en az 6 ayda bir toplanmalıdır.

Toplantılar bilgi güvenliği kapsamında en az aşağıdaki konuları içerecek şekilde planlanmalıdır.
Mevcut durum tespitleri (SBYS kesinti süreleri, nedenleri vb.),
Risklerin planlanması ve analizi,
Tanımlı kullanıcılar için yapılan yetki değişikliklerinin izlenmesi vb,
SBYS'ler üzerinden hastalara ve çalışanlara hangi SMS lerin atıldığı, hangi SMS lerin ulaştığı vb. logların analizi.

Ekip tarafından gerekli görülürse iyileştirici faaliyet çalışmaları başlatılmalıdır.

GD.13.2. Sunucuların güvenliğini sağlamaya yönelik fiziksel düzenleme yapılmalıdır.

- Sunucuların güvenliğini sağlamaya yönelik fiziksel düzenleme en az aşağıdaki parametreleri içerecek şekilde yapılmalıdır:
- Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.
- Yükseltilmiş zemin üzerinde konumlandırılmalı ve tavan asma tavan olmalıdır.
- Yetkili olmayan kişilerin girişini engelleyecek şekilde düzenleme yapılmalıdır.
- Su, yangın, elektrik kesintileri gibi acil durumlara yönelik önlemler alınmış olmalıdır.
- Klima yedeği ile bulunmalıdır.
- Sıcaklık ve nem kontrolleri “Veri Merkezi Kullanılabilirlik TIER 1 Seviyesi”ne göre: Sıcaklık; 18-22 °C, nem ise; %45- %70 aralığında olmalı ve ölçümler kayıt altına alınmalıdır.
- Sunucu odalarında mümkünse pencere olmamalı var ise pencere açılabilir nitelikte olmamalı ve film ile kaplı olmalıdır.
- Sunucu odalarında duman detektörleri; yükseltilmiş zeminin olduğu odalarda zeminin altına, alçaltılmış tavanın olduğu odalarda tavanın üstüne yerleştirmeli ve bunların kontrolleri düzenli olarak yapılarak kayıt altına alınmalıdır.
- Sunucu odalarında güvenlik kamerası bulunmalıdır.

GD.13.3. Sağlık tesisinde Sağlık Bilgi Yönetim Sistemi (SBYS) üzerinde, hasta bilgilerine ilgisiz ve yetkisiz kişilerin erişimini engelleyecek düzenlemeler ile bilgisayar kullanıcılarının hangi alanlara ulaşabileceğine dair yetki tanımlaması yapılmalı ve uygulanmalıdır. Yetki ve erişim, hastaneye yeni gelen ve ayrılan çalışanları da kapsamalıdır.

- Sağlık tesisinde SBYS üzerinde, hasta bilgilerine ilgisiz ve yetkisiz kişilerin erişimini engelleyecek düzenlemeler ile bilgisayar kullanıcılarının hangi alanlara ulaşabileceğine dair yetki tanımlaması yapılıp yapılmadığı ve uygulama ile örtüşüp örtüşmediği değerlendirilmelidir. Hastaneye yeni gelen çalışana yetki tanımlamasının yapılıp yapılmadığı incelenmelidir. Sağlık Hizmetleri Sınıfı dışındaki meslek grubundakiler tarafından SBYS üzerinde hasta bilgilerinin görülmesi konusunda kısıtlama bulunmalıdır.
- Hastaneden ayrılan bir personelin yetki tanımlaması ve sisteme giriş yapıp yapamadığı sorgulanmalıdır.

İŞE BAŞLAMA VE İŞTEN AYRILMA SÜREÇLERİ

HİZMETE ÖZEL

T.C. SAĞLIK BİLGİ SİSTEMLERİ GENEL MÜDÜRLÜĞÜ

İŞE BAŞLAMA FORMU

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.FR.020	31.03.2014	16.11.2015	2	1 / 1

Adı, Soyadı	
Unvanı	
Birimi	
Başlama Tarihi	...../...../20.....

Tamamlanması Gereken Başlıklar	İlgili Birim / Kişi	Kurum Çalışanı İsim-Soyisim /İmza	İşe Başlayan Kişi İsim-Soyisim /İmza
Tanışma ve Kurum Hakkında Genel Bilgi Verilmesi	İnsan Kaynakları Birimi		
Kimlik Kartının Çıkarılması	İnsan Kaynakları Birimi		
Oryantasyon Eğitimi	Eğitim Hizmetleri Birimi		
E-posta Hesabının Açılması	Kullanıcı Hesapları Yönetimi ve Güvenliği Koordinatörlüğü		
BGYS Farkındalık Eğitimi	BGYS Birimi		
EBYS Açılması	EBYS Birimi		
EBYS Eğitimi	EBYS Birimi		
Zimmet Oluşturulması	Taşınır Kayıt Kontrol Birimi		
Personel Gizlilik Sözleşmesi İmzalatılması	Birim Sorumlusu		

HİZMETE ÖZEL

T.C. SAĞLIK BİLGİ SİSTEMLERİ GENEL MÜDÜRLÜĞÜ

İŞTEN AYRILMA FORMU

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.FR.21	31.03.2014	16.11.2015	2	1 / 1

Adı, Soyadı	
Unvanı	
Birimi	
İşten Ayrılma Tarihi	...../...../20.....

Tamamlanması Gereken Başlıklar	İlgili Birim / Kişi	Kurum Çalışanı İsim-Soyisim /İmza	İşten Ayrılan Kişi İsim-Soyisim /İmza
Yaptığı İş ve İşlemlerle İlgili Dokümantasyon ve Bilgilendirme Devri Yapılması	Birim Sorumlusu		
VPN Hesaplarının Kapatılması	Ağ Yönetimi ve Güvenliği		
E-posta Hesabının Kapatılması ve İlgili E-posta Gruplarından Çıkartılması (Danışman, Firma Personeli ve Emekli Olanlar İçin Hesap kapatılmalıdır.)	Kullanıcı Hesapları Yönetimi ve Güvenliği Koordinatörlüğü		
EBYS Kapatılması	EBYS Birimi		
Zimmet Devri	Taşınır Kayıt Kontrol Birimi		
Yemekhane Kartı İptali	Yönetim Hizmetleri Genel Müdürlüğü		
Kimlik Kartının İade Edilmesi	İnsan Kaynakları Birimi		
Veri tabanı yetkilerinin iptali			

GD.13.4. Veri paylaşımı yapılan firmalar ile (SBYS, Laboratuvar hizmet alımları, Görüntüleme hizmet alımları gibi) "Kurumsal Gizlilik Sözleşmesi" yapılmalıdır.

!!!!ŞARTNAMELER !!!!

- Veri paylaşımı yapılan firmalar ile (SBYS, Laboratuvar hizmet alımları, Görüntüleme hizmet alımları gibi) "Kurumsal Gizlilik Sözleşmesi" yapılma durumu değerlendirilmelidir. Yapılan sözleşme, Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından yayınlanan asgari şartları içermelidir.

GD.13.5. Sağlık tesisinde 657 sayılı Devlet Memurları Kanununa tabi personele “Bilgi Güvenliği Farkındalık Bildirgesi” tebliğ edilmeli, kuruma ait gizli bilgilere erişim ihtiyacı olan diğer personel ile "Personel Gizlilik Sözleşmesi" yapılmalıdır.

- T.C. Sağlık Bakanlığı bünyesinde görev yapan 657 Sayılı Devlet Memurları Kanununa tabi personelin, hizmetin ifası esnasında veya herhangi bir gerekçeyle vâkıf oldukları, kuruma ait gizli kalması gereken bilgilerin, gizliliğinin sağlanması ve ifşa edilmemesi için uyulması gereken kuralları tanımlandığı bildirge personele tebliğ edilmelidir. Bildirge, Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından yayınlanan asgari şartları içermelidir. Kuruma ait gizli bilgilere erişim ihtiyacı olan 657 Sayılı Devlet Memurları Kanununa tabi personel haricindeki diğer personeller ile (SBYS, Laboratuvar hizmet alımları, Görüntüleme hizmet alımları, danışman, firma personeli gibi) Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından yayımlanmış "Personel Gizlilik Sözleşmesi" nin yapılma durumu değerlendirilmelidir. Sözleşmenin fotokopilerinin de görülmesi yeterlidir.

Gizlilik Sözleşmeleri

- BG.SZ.01 PERSONEL GİZLİLİK SÖZLEŞMESİ
- BG.SZ.02 KURUMSAL GİZLİLİK TAAHHÜTNAMESİ
- BG.SZ.04 BİLGİ GÜVENLİĞİ FARKINDALIK BİLDİRGESİ
- BG.PR.23 GİZLİLİK SÖZLEŞMELERİ UYGULAMA PROSEDÜRÜ

T.C. SAĞLIK BAKANLIĞI
BİLGİ GÜVENLİĞİ FARKINDALIK BİLDİRGESİ

1. AMAÇ:

Bu bildirge; T.C. Sağlık Bakanlığı bünyesinde görev yapan 657 Sayılı Devlet Memurları Kanununa tabi personelin, hizmetin ifası esnasında veya herhangi bir gerekçeyle vâkıf oldukları, kuruma ait gizli kalması gereken bilgilerin, gizliliğinin sağlanması ve ifşa edilmemesi için uyulması gereken kuralları tanımlar.

2. KAPSAM:

Bu bildirge, Kurum bünyesinde görev yapan 657 Sayılı Devlet Memurları Kanununa tabi personel için hazırlanmıştır. Kuruma ait gizli bilgilere erişim ihtiyacı olan diğer personel (danışman, firma personeli vb.) için Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından yayımlanmış **"BG.SZ.01 Personel Gizlilik Sözleşmesi"** hükümleri uygulanır.

3. YASAL DAYANAK:

Bu bildirge, 657 Sayılı Devlet Memurları Kanununun Gizli Bilgileri açıklama yasağı başlıklı 31'nci maddesine ve 31/12/2015 tarihli Sağlık Bakanlığı Bilgi Güvenliği Yönergesine istinaden hazırlanmıştır.

PERSONEL GİZLİLİK SÖZLEŞMESİ

Bu sözleşme ..... / … / 20… tarihinde, aşağıda yer alan hükümler çerçevesinde, T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü (Genel Müdürlük) ile aşağıda kimlik bilgileri yazılı kişi (Personel) arasında akdedilmiştir.

1. TANIMLAR:

Kuruma Ait Gizli Kalması Gereken Bilgiler:

1.1 Kurum tarafından işlenen (24/3/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan) kişisel veriler ile (20/10/2016 tarih ve 29863 sayılı Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik ile tanımlanan) kişisel sağlık verileri.

1.2 T.C. Sağlık Bakanlığının 24/4/2013 tarih ve 18805 sayılı oluru ile yürürlüğe giren Elektronik Belge Yönetim Sistemi (EBYS) Yönergesi Md. 11 kapsamında tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belge.

1.3 Açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya kuruma haksız yarar sağlama ihtimali bulunan her türlü bilgi ve belge.

GD.13.6. Bilgi Güvenliği ve mahremiyetine yönelik sağlık tesisi çalışanlarına eğitim verilmeli, kayıtları tutulmalı ve SBYS uygulamaları ve güncelleştirmeleri hakkında çalışanlara bilgilendirme yapılmalıdır.

- Bilgi güvenliği ve mahremiyetine yönelik sağlık tesisi çalışanlarına eğitim verildiğine dair kayıtlar incelenmelidir. SBYS uygulamaları ve güncelleştirmeleri hakkında çalışanlara bilgilendirme yapılmalıdır.

GD.13.7. Bilgi Güvenliği ile ilgili risklerin planlanması yapılmalıdır.

- WEB sitesinin hacklenme durumu,
- Yedekleme sırasında sorunlar çıkarsa nasıl geri dönüleceği
- Yazılım ve donanımla ilgili sorunlar,
- Bilgi güvenliği ve mahremiyeti,
- Kullanıcı hataları,
- Veri kaybı,
- Alım süresi ve dolum yüzdesi göz önüne alınarak serverların kapasite planlaması,
- Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler gibi yedekleme kapasitesi artış gereksinimi vb konular ile sbys' ne giriş yapma imkânı olmadığında kimin, hangi kayıtları, nereye, kaydedeceği ve sonrasına yönelik eylem planının nasıl olacağı ve çalışanların konu hakkındaki bilgilendirilmesini içerir.
- Bu risklerin nasıl yönetilmesi gerektiği ile ilgili planlama yapılmalıdır.

GD.13.8. SBYS üzerindeki verilerin yedeklemesi yapılmalıdır.

- Yedekleme sadece sorumlu personel tarafından yapılmalıdır.
- Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgileri ve kurumsal veriler günde en az 3 defa yedeklenmeli ve bu işlem için sistemin yoğun olmadığı zamanlar seçilmelidir.
- Yedekler, SBYS' nin bulunduğu sunucu dışında bir ortama alınmalıdır. Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak manyetik kartuş, harici bellek, DVD, disk, CD vb. ortamda yedekleri alınmalıdır. Taşınabilir ortamlar (harici bellek, manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda saklanmalıdır. Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
- Yedekleme ortamlarının ve yedeklenmiş verinin düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması için yılda bir kez "veri kurtarma testi" yapılmalı gerekli ise iyileştirme çalışmaları başlatılmalıdır.

GD.13.9. SBYS'ye izinsiz erişimler engellenmelidir.

.

- Dış ortamdan iç ortama hangi durumda kimler tarafından erişim yapılacağı belirlenmelidir. Erişim yetkisi verilen kişi haricinde erişim sağlanmamalıdır. Erişimin ne zaman, kimin tarafından, ne için, hangi alanda yapıldığı gibi bilgiler kayıt altına alınmalıdır.
- Her bilgisayara merkezi sunucu tarafından kontrol edilebilen antivirüs yazılımı kurulmalı ve bu yazılım kullanıcılar tarafından pasif hale getirilmemelidir.
- Sunucular güvenlik duvarının arkasında bulunmalıdır.
- Koruma amaçlı kullanılan yazılımlar güncel olmalıdır.

GD.13.10. SBYS kesinti süreleri, nedenleri ve arıza durumları kayıt altına alınmalı ve gerekli ise iyileştirme çalışmaları yapılmalıdır.

- Sistem üstünden yada formlar üzerinden kontrol edilebilir.

GD.13.11. SBYS' de Parola güvenliğine yönelik düzenleme yapılmalıdır.

- SBYS ekranı üzerinde yapılan kontrolde;
- Parola en az 8 karakterden oluşmalıdır.
- Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içermelidir.
- Büyük ve küçük harfler bir arada kullanılmalıdır.
- Yukarda yazılan kurallara aykırı parola oluşturduğunda sistem kabul etmemeli ve parola için değişim süresi belirlenmeli ve bu süreye uyum gösterilmelidir.

Parola Güvenliği

Parolaların kırılma süresi

Parola: Muhteşem

Çözülme süresi: 9.08 dakik

Parola: Muhteşem8

Çözülme süresi: 1.59 gün

12

Parola: Muht+e$em8

Çözülme süresi: 19 yıl

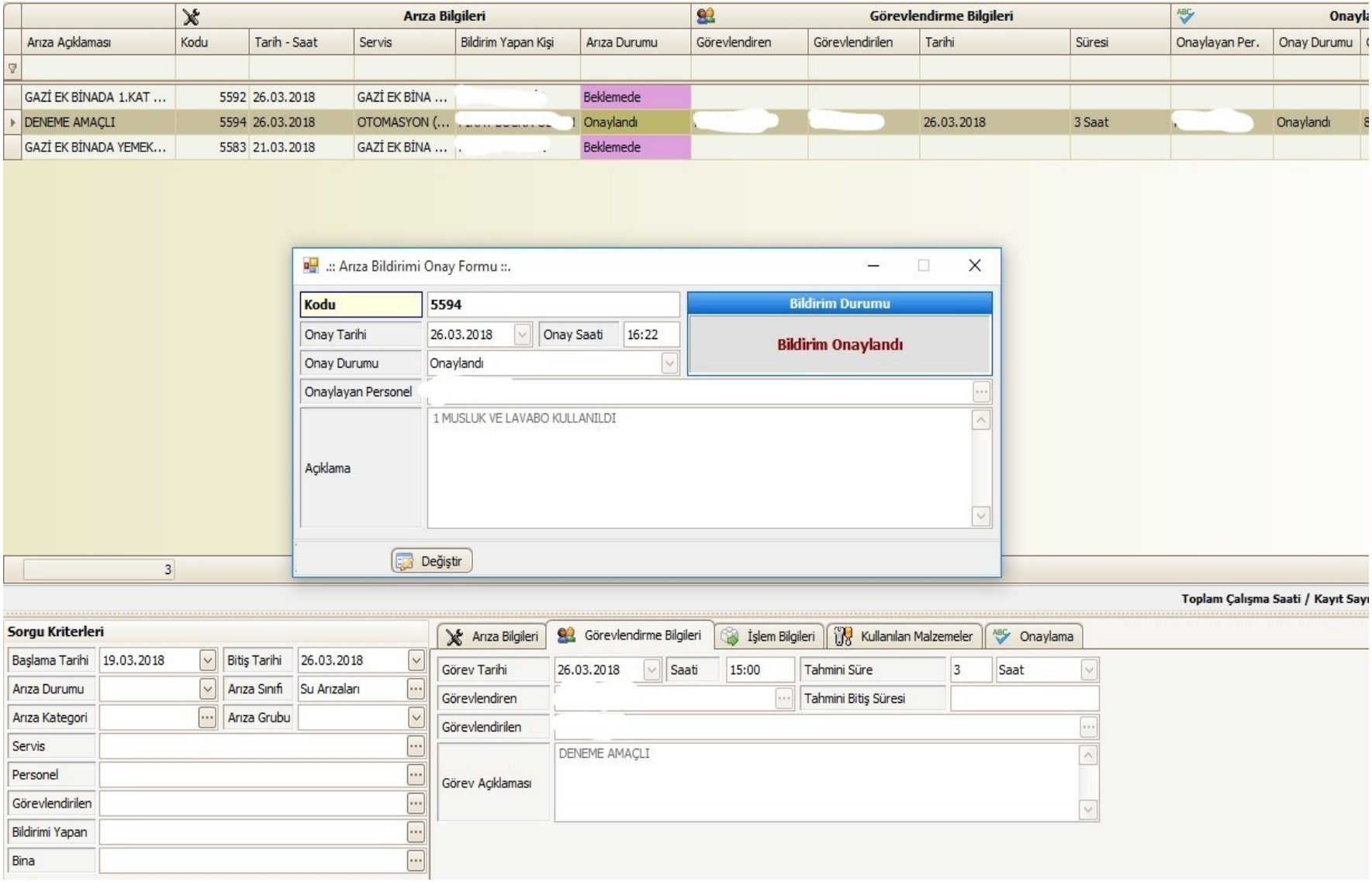
Parola: Muh50te$8em+

Çözülme süresi: 17,400,000 yıl

Parolanızı test etmek için
http://www.bilgimikoruyorum.org.tr/?b223_yaparak_ogrenelim

GD.13.12. SBYS üzerinde Teknik Servis Yönetim modülü oluşturulmalı, arıza ve tamirlere ilişkin süreçlerin yönetimi bu modül üzerinden yapılmalıdır (C, D ve E1 grubu hastaneler muaftır).

- SBYS, Bilgi işlemle ilgili (network, donanım, office dosyaları, antivirüs taraması vb.) ve diğer arızalara (elektrik, su, teçhizat, tesisat vb.) ilişkin süreçlerin izlenebilmesi SBYS üzerinden yapılmalıdır. Hastane mevcut arızalarını tanımlayarak her arıza için mevcut personel, hastane büyüklüğü, cihaz sayısı ve çeşitliliği gibi faktörleri göz önünde bulundurarak arızaların giderilmesi için hedef süre belirlemelidir. Kullanıcının arıza kaydı oluşturduğu, arıza kaydının ilgili birim tarafından alındığı ve çözüme ulaştığı tarih saat ve talebi takip eden kişi sistemden izlenebilmelidir. Hastanenin belirlemiş olduğu hedefler, uyum durumu hastane yönetimi tarafından incelenmelidir. Biyomedikal cihaz arıza bildirimi olduğunda, biyomedikal depoya bu bilgi sistem üzerinden aktarılmalı ve cihaz arızalı/pasif olarak gözükmelidir.


Arıza Bilgileri
Görevlendirme Bilgileri
Onayla
Arıza Açıklaması
Kodu
Tarih - Saat
Servis
Bildirim Yapan Kişi
Arıza Durumu
Görevlendiren
Görevlendirilen
Tarihi
Süresi
Onaylayan Per.
Onay Durumu
GAZİ EK BİNADA 1.KAT ...
5592
26.03.2018
GAZİ EK BİNA ...
Beklemede
DENEME AMAÇLI
5594
26.03.2018
OTOMASYON (...
Onaylandı
26.03.2018
3 Saat
Onaylandı
GAZİ EK BİNADA YEMEK...
5583
21.03.2018
GAZİ EK BİNA ...
Beklemede
:: Arıza Bildirimi Onay Formu ::.
Kodu
5594
Bildirim Durumu
Onay Tarihi
26.03.2018
Onay Saati
16:22
Bildirim Onaylandı
Onay Durumu
Onaylandı
Onaylayan Personel
Açıklama
1 MUSLUK VE LAVABO KULLANILDI
Değiştir
3
Toplam Çalışma Saati / Kayıt Sayı
Sorgu Kriterleri
Başlama Tarihi
19.03.2018
Bitiş Tarihi
26.03.2018
Arıza Durumu
Arıza Sınıfı
Su Arızaları
Arıza Kategori
Arıza Grubu
Servis
Personel
Görevlendirilen
Bildirimi Yapan
Bina
Arıza Bilgileri
Görevlendirme Bilgileri
İşlem Bilgileri
Kullanılan Malzemeler
Onaylama
Görev Tarihi
26.03.2018
Saati
15:00
Tahmini Süre
3
Saat
Görevlendiren
Tahmini Bitiş Süresi
Görevlendirilen
Görev Açıklaması
DENEME AMAÇLI

GD.13.13. SBYS üzerinde oluşturulan “Personel Yönetim modülü”nde çalışan personelin TC kimlik numarası, ünvanı, çalıştığı birim, varsa sertifikası, iletişim bilgileri (telefon , mail vb.) güncel olmalıdır.

GD.37.1 Görevli hekim poliklinik hizmet sürecinde hastalara ait tıbbi bilgilere SBYS ekranında bulunan e-Nabız butonu üzerinden erişim sağlayabilmelidir.

GD.37.2 e-Nabız butonu SBSGM tarafından yayımlanan standartlara uygun olmalıdır.

- -e-Nabız butonu e-Nabız sistemine ait güncel logo olmalıdır.
- -Buton hekimlerin ilk anda görebileceği alanda bulunmalıdır.
- -Butonun üzerine gelindiğinde “Hastanın sağlık geçmişini görüntülemek için tıklayınız.” ibaresi yer almalıdır.

GD.37.3 Hastalara ait görüntüleme verilerine PACS üzerinden erişim sağlanmalıdır.

- Hekimler polikliniklerde ve servislerde hastalarına ait tüm görüntüleme verilerine kullandıkları SBYS üzerinden erişim sağlayabilmelidirler.

KURUM_AL

GÜV_ _LİK

S E N *'siz Olmaz!*

TÜBİTAK

SGE

TEŞEKKÜR EDERİM

Dilek ŞEN KARAKAYA
Sağlık Bilgi Sistemleri Genel Müdürlüğü
Bilgi Güvenliği Yönetim Sistemleri Birim Sorumlusu

dilek.karakaya@saglik.gov.tr