BGYS POLİTİKASI

BGYS politikası, **T.C. Sağlık Bakanlığı Ankara İl Sağlık Müdürlüğü ve Bağlı Birimler** bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır. Bu politikada tüm bölümleri ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır.

1. AMAÇ

Bu politika; Ankara İl Sağlık Müdürlüğünde tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamak ve kurumun dışardan veya içeriden gelebilecek, kasıtlı veya kasıtsız oluşabilecek tüm tehditlerden korunması, kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve bilginin geniş çaplı tehditlerden korunmasını sağlamak amacıyla hazırlanmıştır. Bilgi; diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat Kurum açısından en önemli varlıklardan biridir. Bilgi Güvenliği; Ankara Sağlık Müdürlüğü ve bağlı birimlerinin sahip olduğu bilgi varlıklarının korunması ve uygun biçimde yönetilmesinin sağlanmasıdır.

2. HEDEF

Bilgi Güvenliği Politika şartlarını yerine getirerek, çalışanların bilgi güvenliği farkındalığını arttırmak, teknik güvenlik kontrollerini uygulamak ve kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak (iş sürekliliği), kurumsal riskleri en alt seviyeye indirerek kurumun güvenliği ile güvenilirliğini ve temsil ettiği kurumun imajını korumaktır.

3. KAPSAM

"Bilgi Güvenliği Yönetim Sistemleri Politikası" dokümanında yer alan kriterler, Ankara İl Sağlık Müdürlüğü ve bağlı birimlerinde, çalışan tüm personel ile aşağıdaki varlık ve teknoloji kategorilerini kapsamaktadır.

a) Veri dosyaları, sözleşmeler ve benzeri tüm bilgi varlıkları,

b) Uygulama ve Sistem Yazılımları,

c) Güvenlik cihazları, sunucular (server),

d) Bilgisayarlar, iletişim donanımı ve veri depolama ortamları,

e) Tüm işlevlerin yerine getirilmesi için gerekli fiziksel varlıklar (aydınlatma, iklimlendirme, kablolama vs.),

f) Kurum tarafından üretilen, kullanılan ve geliştirilen tüm verileri kapsar.

4. DAYANAK

- 21/06/2019 tarihli ve 30808 sayılı Resmi Gazetede yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik (Yönetmelik)
- 02/05/2018 tarihli ve 98813799.719.54 sayılı Bakanlık Makam onayı ile yürürlüğe giren Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi (Yönerge)
- Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu (Sürüm 2.1) (Kılavuz)
- Sağlık Bakanlığı Kurumsal SOME Kurulum ve Yönetim Rehberi (Rehber)
- Cumhurbaşkanlığı tarafından yayımlanan 2019/12 sayılı "Bilgi ve İletişim Güvenliği Tedbirleri" hakkında genelge.

5. TANIMLAR ve KISALTMALAR

- **Ankara İl Sağlık Müdürlüğü:** Ankara İl Sağlık Müdürlüğü, Başkanlıklarını, şubelerini ve tüm birimlerini ifade etmektedir.
- **Bağlı Birimler:** İlçe Sağlık Müdürlükleri ile 112 Komuta Kontrol Merkezi ve Acil Sağlık Hizmetleri İstasyonlarını (ASHİ) ifade etmektedir.
- **Varlık:** Ankara İl Sağlık Müdürlüğü iş süreçleri için değeri olan, kaybı halinde işlerin aksayacağı, insan, yazılım, donanım, itibar, bilgi gibi unsurların tümüdür.
- **Gizlilik:** Bilginin sadece yetkili kişiler tarafından erişilebilir olmasıdır.
- **Bütünlük:** Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılmasıdır.
- **Erişilebilirlik:** Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an erişilebilir olmasıdır.
- **Bilgi Güvenliği:**Bilgi ve bilgi işleme tesislerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz şahısların bilgiye ulaşmaları halinde tespit

edilmelerine yönelik tedbirlerin tümüdür.

- **Bilgi Güvenliği İhlal Olayı:** İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.
- **Bilgi Güvenliği Yönetim Sistemi (BGYS) :** Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir.
- **İSM**: İl Sağlık Müdürlüğü
- **SOME:** Siber Olaylara Müdahale Ekibi
- **Üst Yönetim:** Kurum adına karar verme ve harcama yetkisine sahip yönetici / yöneticilerdir.

6. BİLGİ GÜVENLİĞİ HEDEFLERİ VE PRENSİPLERİ

6.1 Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir. Her bir varlık için risk seviyesinin kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir.

6.2 Risk yönetimi ve kontrollerin uygulanması sürekli bir faaliyettir ve kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılması hedeflenmektedir.

7. BİLGİ GÜVENLİĞİ ORGANİZASYONU

7.1 İSM genelinde (Müdürlüğe bağlı olan tüm sağlık teşkillerini de kapsayacak şekilde) bilgi güvenliği ve siber olaylara müdahale ile ilgili konularda en üst düzeyde karar organı olarak görev yapmak, bilgi güvenliği yetkilisi ve kurumsal SOME tarafından gerçekleştirilecek faaliyetlere destek vermek, Bakanlık tarafından yayımlanan eylem planları doğrultusunda bilgi güvenliği ile ilgili faaliyetleri takip etmek ve gerekli çalışmaları yapmak maksadıyla **İSM Bilgi Güvenliği Alt Komisyonu** oluşturulmuştur.

7.2 Bilgi Güvenliği Alt Komisyonu çalışmalarını koordine etmek ve komisyon toplantılarına başkanlık yapmak üzere İSM'de görev yapan bir personel **Bilgi Sistemleri Koordinatörü**olarak atanmıştır.

Hazırlayan	Kontrol Eden	Onaylayan
Fulya KIZILKUŞ Bilgi Güvenliği Yetkilisi	Osman BAHÇEKAPILI Destek Hizmetleri BaşkanYard. Bilgi Sistemleri Koordinatörü	Mehmet GÜLÜM İl Sağlık Müdürü

7.3 Yönerge ve Kılavuzda belirtilen görevleri yerine getirmek ve İSM bünyesinde yer alan tüm kurum ve kuruluşlar adına Sağlık Bilgi Sistemleri Genel Müdürlüğü ile koordineli olarak gerekli çalışmaları yürütmek üzere **Bilgi Güvenliği Yetkilisi**ve **Kurumsal SOME Ekip Lideri** görevlendirilmiştir.

7.4 İlimiz genelinde meydana gelebilecek siber olaylara müdahale etmek ve görev alanı ile ilgili hususlarda Bakanlık Sektörel SOME ile birlikte çalışmak üzere, Rehberde belirtilen esaslar çerçevesinde bir adet Kurumsal SOMEoluşturulmuştur.

7.5 Bilgi güvenliğinin insan kaynakları, fiziksel ve çevresel güvenlik, hukuk işleri ve bilgi sistemleri ile ilgili alanlarında gerekli desteği vermek üzere ilgili birimleri temsilen Bilgi Güvenliği Alt Komisyonunda komisyon üyesi olarak görev yapmak üzere personel görevlendirmesi yapılmıştır.

7.6 Yukarıda belirtilen esaslar doğrultusunda İl Sağlık Müdürü oluru ile görevlendirilmiş personel bilgileri ektedir.

7.7 İSM' ye bağlı diğer sağlık tesislerinde bilgi güvenliği ile ilgili faaliyetler aşağıda belirtilen usul ve esaslar doğrultusunda yürütülür.

7.7.1. İSM' ye bağlı 2 ve 3'ncü basamak sağlık hizmeti sunumu yapan sağlık teşkillerinde bilgi güvenliği ile ilgili faaliyetleri yürütmek ve İSM Bilgi Sistemleri Koordinatörü, İSM Bilgi Güvenliği Yetkilisi ve Kurumsal SOME Lideri ile her türlü koordinasyonu yapmak üzere bir personel Bilgi Güvenliği Yetkilisi olarak görevlendirilir. Bilgi Güvenliği Yetkilisi görevlendirilmesi yapılırken mümkün olması halinde ilgili kurumda günlük bilgi sistem işletme ve yönetim faaliyetlerini yapmakla sorumlu personel dışında, Kılavuz'un A.2.4.3 maddesinde belirtilen niteliklerde bir kişinin seçilmesi tercih edilir.

7.7.2. 2 ve 3'üncü basamak sağlık teşkillerince, gerekiyorsa İSM Bilgi Güvenliği Alt Komisyonu ile benzer görevleri yürütmek üzere Hastane Bilgi Güvenliği Ekibi kurulur. (Kurulması halinde) Bu ekiplerde görev yapan personelin kimlik bilgileri, **Hastane Hizmet Kalite Standartları** gereği hazırlanması gereken **Hastane Bilgi Yönetim Süreç dokümanlarında** belirtilir. Bu personelin bilgilerinin, ayrıca İl Sağlık Müdürlüğüne gönderilmesine gerek bulunmamaktadır.

7.7.3. İSM' ye bağlı 1'inci basamak sağlık hizmeti sunumu yapan sağlık teşkillerinde ayrıca bir bilgi güvenliği yetkilisi görevlendirmesi yapılmaz. Varsa ilgili kurumda günlük bilgi sistem işletme ve yönetim faaliyetlerini yapmakla sorumlu olan kişi bilgi güvenliği ile ilgili faaliyetleri de yürütür. Konuyla ilgili hiçbir personeli olmayan kurum ve kuruluşların bilgi güvenliği ile ilgili faaliyetleri İSM Bilgi Güvenliği Yetkilisi tarafından yerine getirilir.

7.8 İSM Kurumsal SOME' si, İSM' nin kendisi de dâhil İSM' ye bağlı tüm sağlık teşkillerinde meydana gelen siber güvenlik olaylarına müdahale etme ile yetkilidir. Diğer sağlık teşkillerinde bu ad altında bir ekip ya da kişi görevlendirilmesi yapılmasına gerek bulunmamaktadır.

1. BGYS Alt Komisyonu

- Destek Hizmetleri Başkanlığı Başkan Yardımcısı Osman BAHÇEKAPILI
- İstatistik ve Bilgi İşlem Birimi Uzman Emre Çağatay DOĞAN
- İstatistik ve Bilgi İşlem Birimi Uzman Mustafa Atilla IŞIK
- İstatistik ve Bilgi İşlem Birimi Mühendis (Bilgisayar) Fulya KIZILKUŞ
- İstatistik ve Bilgi İşlem Birimi Programcı Özcan ŞİŞMAN
- İstatistik ve Bilgi İşlem Birimi Sistem Yöneticisi Orhan Kemal AKARDENİZ
- İstatistik ve Bilgi İşlem Birimi VHKİ Gözen OKUR KOYUNCU
- Satın Alma Birimi Uzman Serkan ESEN
- Uzman Yasemin ÖZÇELİK
- Personel Hizmetleri Başkanlığı Uzman Tayfun POLAT
- Personel Hizmetleri Başkanlığı Uzman Hayrettin ÖZKAN
- Koruma ve Güvenlik Birimi Birim Sorumlusu Şevki ERDOĞAN
- Koruma ve Güvenlik Birimi Erkan ÖZDEMİR
- Kalite Koordinatörlüğü Uzman Elif Gamze BUDAK

2. BGYS Komisyonu Görev, Yetki ve Sorumluluklar:

- Bilgi güvenliği politika ve stratejilerini belirler, gerektiğinde Bilgi Güvenliği Politikaları Yönergesine bağlı olarak hazırlanacak olan kılavuzlarla ilgili revizyon kararlarını verir,
- Bilgi güvenliği politikalarının uygulamasının etkinliğini gözden geçirir,
- Bilgi güvenliği faaliyetlerinin yürütülmesini yönlendirir,
- Bilgi güvenliği eğitimi ve farkındalığını sağlamak için plan ve programları hazırlar,
- Bilgi güvenliği faaliyetleri ve kontrollerinin tüm kurum ve kuruluşlarda koordine edilmesini sağlar.
- Yürütülen çalışmaların tabana yayılması hususunda planlanan çalışmalara katılır, bağlı oldukları birimlerde bu çalışmaların yayılmasına öncülük eder,

8. BİLGİ HASSASİYETİ VE RİSKLER

8.1 Bilgi Varlıklarımız

- T.C. Sağlık Bakanlığı Ankara İl Sağlık Müdürlüğü Başkanlıkları ve Bağlı Kuruluşlarbünyesinde Madde 3 te belirtilen kapsam dahilinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları işlerde üretilen bilgiler bilgi varlıklarımızı oluşturmaktadır.
- Masaüstü bilgisayarlar, laptoplar, tabletler, telefonlar, CD, DVD, Digital Veri Depolama Alanları ve USB Bellek ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (internet, email, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

8.2 Varlık Sınıflandırılması

BİLGİ SINIFLANDIRMA KILAVUZU		Saklanma Yeri
Çok Gizli	En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır	Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar , digital depolama alanları.
Gizli	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır	Departmanın kilitli dolapları, digital depolama alanları.
Özel	Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kurum işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, Laptop veya Dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişilebilirlik ön plandadır	Çalışma masalarının kilitli çekmeceleri
Hizmete Özel	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın kilitli ortak dolapları
Tasnif Dışı	Bu bilgiler T.C. Sağlık Bakanlığına bağlı tüm teşkilatına, tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Dolaplar ve dolap dışlarında

- Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmalıdır. Bu sınıflandırmaya göre halka açık dokümanlar web sitesinde yayınlanan ve işlem için üçüncü taraflara verilen kağıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

9. POLİTİKA METNİ

9.1 Ankara ISM bilgi güvenliği modeli, Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzuna dayanır ve kurumsal bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak için operasyonel ve yönetsel çerçeveyi sunar.

9.2 Ankara İl Sağlık Müdürü, üst yönetim adına, kurumsal faaliyetlerin icrasında iş süreçlerinin bilgi güvenliği kurallarına uygun olarak yürütülmesi için gerekli olan kaynak ihtiyaçlarını temin etmek ve bilgi güvenliğinin etkin bir şekilde uygulanmasını sağlamak hususundaki iradesini, Bilgi Güvenliği Taahhütnamesi ile taahhüt ve beyan etmiştir. Taahhütname, ankara.ism@saglik.gov.tradresinde yer almaktadır.

9.3 Tüm personel, faaliyetlerini dayanak kısmında belirtilen mevzuat ve başta bu politika olmak üzere üst yönetim tarafından belirlenen bilgi güvenliği politikalarına uygun şekilde yürütmekten sorumludur.

9.4 Tüm personelankara.ism@saglik.gov.tradresinde yayımlanmış olan BGYS politikalarını bilmek ve gerekliliklerini uygulamakla sorumludur.

9.5 Bilgi güvenliği ihlal olayı fark edildiğinde, https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir adresinde yer alan ihlal bildirimi internet sayfası aracılığı ile bildirilmesi tüm personelin sorumluluğundadır.

9.6 Fiziksel güvenlik tedbirleri çerçevesinde (giriş çıkış kapıları, ofis odaları, ürün teslim alanları, depoların güvenliği ve personel tanıtım kartlarının kullanımı vb.) belirlenmiş kurallara tüm personel tarafından uyulması zorunludur.

9.7 Bilişim altyapı hizmetlerine erişmek isteyen (sunucu erişimi, veri tabanı erişimi vb.) dış taraflar (erişime ihtiyaç duyan her türlü tedarikçi ya da Sağlık Bakanlığı dışındaki kurumlar) mutlak suretle kurum erişim prosedürüne uygun bir şekilde erişim sağlamalıdır. Uygunsuz erişim girişimleri ihlal olayı olarak tanımlanır.

9.8 İl Sağlık Müdürlüğüne bilgi güvenliği politikası kapsamında hizmet veren tüm taraflar ile gizlilik sözleşmesi imzalanır.

9.9 Her kullanıcı bilgisayarına, tabletine oturum şifresi koymak zorundadır.

9.10 Tüm kullanıcılar kurumsal işlemlerde resmi olarak tahsis edilen @saglik.gov.tr uzantılı e-posta adresini kullanmak zorundadırlar.

Hazırlayan	Kontrol Eden	Onaylayan
Fulya KIZILKUŞ Bilgi Güvenliği Yetkilisi	Osman BAHÇEKAPILI Destek Hizmetleri Başkan Yard. Bilgi Sistemleri Koordinatörü	Mehmet GÜLÜM İl Sağlık Müdürü

9.11 Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir.

9.12 Bütün kullanıcılar kendi bilgisayarlarının güvenliğinden sorumludur. Açık bırakılması halinde ve ya kullanıcı oturum şifrelerinin ikinci şahıslarca biliniyor olması durumlarında bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) bilgisayarın sahibi sorumludur.

9.13 Kurumun bilgisayarları kullanılarak taciz veya yasadışı olaylara karışılmamalıdır.

9.14 Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packetsniffing, packetspoofing, denial of service vb.) eylemlere girişilmemelidir.

9.15 Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DOS saldırısı, port- network taraması vb. yapılmamalıdır.

9.16 Cihazlar, yazılımlar ve veriler izinsiz olarak kurum dışına çıkarılmamalıdır.

9.17 Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, Kurumumuzun bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kâğıt ortamında üçüncü kişi ve kurumlara verilemez.

9.18 Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programlar (Dergi CD'leri veya internetten indirilen programlar vs.) kurulmamalı ve kullanılmamalıdır. Lisansız yazılımı bilgisayarında barından personel ilgili mevzuat çerçevesinde kendisi sorumludur.

9.19 Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü, dizüstü bilgisayarlarındaki ve tabletlerindeki kurumsal bilgilerin güvenliği ile sorumludur.

9.20 Bilgi İşlem Birimi tarafından yetkili kişiler kullanıcıya haber vermek kaydı ile yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel bağlanılan bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.

9.21 Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.

9.22 Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

Hazırlayan	Kontrol Eden	Onaylayan
Fulya KIZILKUŞ Bilgi Güvenliği Yetkilisi	Osman BAHÇEKAPILI Destek Hizmetleri Başkan Yard. Bilgi Sistemleri Koordinatörü	Mehmet GÜLÜM İl Sağlık Müdürü

9.23 Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir

9.24 Kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde USB flash bellek ve/veya harici hard disk gibi removablemedia (taşınabilir medya) bırakmamalıdır.

9.25 Son kullanıcılar, mesai bitiminde bilgisayarlarını kapatmalıdır.

9.26 Kullanıcı bilgisayarlarında, güncel anti virüs bulunmalıdır.Hiç bir kullanıcı herhangi bir sebepten dolayı anti virüs programını sistemden kaldıramaz ve başka bir anti virüs yazılımını sisteme kuramaz.

9.27 Zararlı programları (virüs, solucan, truva atı, e-mail bombaları vb.)kurum bünyesinde oluşturmak ve dağıtmak yasaktır

9.28 Dizüstü bilgisayarın, tabletlerin veya telefonların çalınması/kaybolması durumunda en kısa sürede Sağlık Müdürlüğü İstatistik ve Bilgi İşlem Birimine haber verilmelidir.

10. İNSAN KAYNAKLARI ZAFİYETİ YÖNETİMİ

10.1. Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.

10.2. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.

10.3. ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında (izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.

10.4. Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.

10.5. İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kağıt kesme makinasında imha edilmelidir.

10.6. Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

10.7. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.

10.8. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

10.9. Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla kartları üreten ilgili şubeye iade

etmelidir.

11. SOSYAL MÜHENDİSLİK ZAFİYETLERİ

İnsanların zafiyetlerinden faydalanarak çeşitli etkileme, ikna ve kandırma yöntemleriyle istenilen (normalde paylaşmamaları gereken) bilgileri elde etmeye çalışmaktır.

11.1. Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.

11.2. Arkadaşlarımızla paylaştığımız bilgileri seçerken dikkat edilmelidir.

11.3. Telefon, e-posta veya sohbet yoluyla yapılan haberleşmelerde Kullanıcı adı ve özellikle şifre bilgileri paylaşılmamalıdır. Şifre kişiye özel bilgidir. Sistem yöneticileri dâhil telefonda veya e-posta yazışmalarında şifremizi paylaşmamalıyız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.

11.4. eMule, torrent gibi dosya paylaşım yazılımları kullanılmamalıdır.

11.5. Sadece yetkili kişilerin kurum içerisindeki sınırlı bölümlere erişim izni olduğundan emin olmak için uygun erişim kontrol mekanizmaları olması gerekir.

11.6. Kurum Web Sayfasında kurum ile ilgili paylaşılan bilgilere son derece dikkat edilmeli ve bu sürekli izlenmelidir.

11.7. Elektronik posta ile yapılan yazışmalarda saglik.gov.tr uzantılı e-posta hesapları kullanılmalıdır.

11.8. E-Postalara gelen kaynağı belli olmayan, şüphe uyandıran e-postalar açılmamalı ve ilgili sorumlulara bilgi verilmelidir.

11.9. Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.

11.10. Kurum içi bilgiler, sosyal medyada paylaşılmamalıdır.

11.11. Kuruma ait hiçbir gizli bilgi ve yazı sosyal medyada paylaşılmamalıdır.

12. BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ

12.1. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.

Hazırlayan	Kontrol Eden	Onaylayan
Fulya KIZILKUŞ Bilgi Güvenliği Yetkilisi	Osman BAHÇEKAPILI Destek Hizmetleri Başkan Yard. Bilgi Sistemleri Koordinatörü	Mehmet GÜLÜM İl Sağlık Müdürü

12.2. Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.

12.3. İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.

12.4. Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.

12.5. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.

12.6. Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.

12.7. Hacimsel küçültme işlemi için parçalanmalıdır.

12.8. Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

13. ŞİFRE KULLANIM POLİTİKASI

13.1. Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

13.2. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

13.3. Şifreler başkası ile paylaşılmamalı, kâğıtlara ya da elektronik ortamlara yazılmamalıdır.

13.4. En az sekiz karakterden oluşmalıdır.

13.5. Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, *, %" gibi özel karakterler içermelidir.

13.6. Büyük ve küçük harfler bir arada kullanılmalıdır.

13.7. Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız vb.)

13.8. Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.(w3rhaba,1iki3 vb.)

13.9. Herhangi bir kişiye telefonda şifre verilmemelidir.

13.10. Şifreler, işten uzakta olunduğu zamanlarda iş arkadaşlarına verilmemelidir.

14. İŞE BAŞLAYIŞ VE İŞTEN AYRILMA PROSEDÜRÜ

a. İşe Başlayış Prosedürü

14.a.1 İşe başlayan her personele (kadrolu ve hizmet alımı dâhil) bilgi güvenliği ve sosyal mühendislik zafiyetleri konularıyla ilgili eğitim verilmelidir.

14.a.2 Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Her çalışan personel "Bilgi Güvenliği Kullanıcı Sözleşmesi"ni (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzalamakla yükümlüdür.

14.a.3 Var ise kullanacağı bilgi sistemlerine yönelik kullanıcı adı ve şifreleri tanımlanmalıdır.

14.a.4 EBYS üzerinden yazışma yapabilmesi ve ya yazışmaları takip edebilmesi için ilgili personele saglik.gov.tr uzantılı e-mail adresi tanımlanmalıdır. İl içi yer değişikliklerinde ise sistem üzerinden kurum/birim değişikliği tanımlaması yapılmalıdır.

14.a.5 Tüm personele kurum kimlik kartı çıkartılmalıdır.

b. İşten Ayrılma Prosedürü

14.b.1 Görevden ayrılan personelin kurum kimlik kartı ve yaka kartı alınmalıdır.

14.b.2 Kullandığı bilgi sistemlerine yönelik (ÇKYS/TSIM, EBYS vb.) kullanıcı adı ve şifreleri ilgili sistem yöneticileri tarafından iptal edilmeli ya da pasif hale getirilmelidir.

14.b.3 Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.

14.b.4 Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

14.b.5 Görevden ayrılan personel "İŞTEN AYRILMA ONAY FORMU" nu doldurarak bağlı bulunduğu kurumun insan kaynakları birimine teslim etmelidir.

14.b.6 İlgili form doldurulmadan personelin kurum ile ilişiği kesilmez.

Hazırlayan	Kontrol Eden	Onaylayan
Fulya KIZILKUŞ Bilgi Güvenliği Yetkilisi	Osman BAHÇEKAPILI Destek Hizmetleri Başkan Yard. Bilgi Sistemleri Koordinatörü	Mehmet GÜLÜM İl Sağlık Müdürü

15. MAL VE HİZMET ALIMI GÜVENLİĞİ

15.1 Kurum olarak mal ve hizmet alımlarında ilgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak rekabeti engellemeyecek şekilde gerekli güvenlik düzenlemeleri Teknik şartnamelerde belirtilmelidir.

15.2 Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; Sorumluluk, geçiş durumu planlama ve işlemler süresince potansiyel kesinti süresi, acil durum planlaması yönetmelikleri ve durum tespitinin gözden geçirilmesi, güvenlik olayları hakkında bilgi toplanması ve yönetimi konularında sorular içerecektir. Bu nedenle, dış kaynaklı bir yönetmelik geçişinde; kuruluş değişiklikleri yönetmek için uygun süreçlere ve anlaşmaların yeniden müzakere edilmesi ya da fesih edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.

15.3 Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.

16. BİLGİ GÜVENLİĞİ DÖKÜMANI VE İHLAL BİLDİRİMİ

Kurum bünyesinde tüm çalışanların genel olarak uyması gereken kurallar doküman olarak hazırlanıp tüm personele dağıtılmıştır. Personel bu dokümanda önerilen uygulamaları takip etmeli, zayıflık ve tehditlere karşı farkında olmalıdırlar. Personel bu dokümanda tanımlanan bilgi güvenliği ihlallerini yapmamalı ve bu ihlalleri gözlemlediğinde mutlaka BGYS Komisyonuna veya http://ankaraism.saglik.gov.tr web adresindeki formu doldurarak bildirmelidirler.

17. BİLGİ GÜVENLİĞİ SÖZLEŞMELERİ

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

18. BİLGİ GÜVENLİĞİ EĞİTİMLERİ

Kurumumuzda yılda bir kez tüm personele farkındalık eğitimi verilecektir. Gerekli görüldüğü hallerde de eğitim tekrarlanacaktır.

Hazırlayan	Kontrol Eden	Onaylayan
Fulya KIZILKUŞ Bilgi Güvenliği Yetkilisi	Osman BAHÇEKAPILI Destek Hizmetleri Başkan Yard. Bilgi Sistemleri Koordinatörü	Mehmet GÜLÜM İl Sağlık Müdürü

19. EKLER

19.1 Tüm Sağlık Teşkilleri Tarafından Ortak Olarak Kullanılacak Destek Dokümanları:

- İSM Bilgi Güvenliği Organizasyonda Görev Yapan Personel Bilgileri
- Parola Politikası
- Erişim Kontrol Prosedürü ve Erişim Kontrol Matrisleri (merkezi olarak kullanılan sistemler ve SBYS yazılımları için)
- Uzaktan Erişim Prosedürü (VPN Bağlantı Talep Formu vb. dâhil)
- Bilgi Saklama Ortamları Yok Etme Prosedürü
- İnternet ve E-Posta Kullanım Politikası
- Sosyal Medya ve Sosyal Mühendislik Saldırılarından Korunma Politikası

19.2 Sağlık Teşkilleri Tarafından Kendi Kurumlarına Özgü Hazırlanması Gereken Destek Dokümanları:

- Fiziksel ve Çevresel Güvenlik Prosedürü
- Erişim Kontrol Prosedürü ve Erişim Kontrol Matrisleri (yerel olarak kullanılan sistemler ve özellikle SBYS yazılımları için)
- Varlıkların Kabul Edilebilir Kullanımı Prosedürü (Taşınabilir Ortam Yönetimi ile İlgili Konular Dâhil)
- Temiz Masa, Temiz Ekran Talimatı
- İşe Başlama, Görev Değişikliği ve İşten Ayrılma Prosedürü (İşe Başlama Formu, İşten Ayrılma Formu vb. dâhil)
- Yedekleme Prosedürü
- Sistem Güvenlik Prosedürü (Etki Alanı, Sunucu ve Sistem Odası Güvenliği, Ağ Güvenliği, Zararlı Yazılımlardan Korunma vb. hususları içerecek şekilde)

Hazırlayan	Kontrol Eden	Onaylayan
Fulya KIZILKUŞ Bilgi Güvenliği Yetkilisi	Osman BAHÇEKAPILI Destek Hizmetleri Başkan Yard. Bilgi Sistemleri Koordinatörü	Mehmet GÜLÜM İl Sağlık Müdürü