Bilgi Güvenliği

İZMİR İL SAĞLIK MÜDÜRLÜĞÜ

2018

GİRİŞ

Bilgi Güvenliği Politikaları Kılavuzunda belirtildiği üzere; Bilgi Güvenliği ile ilgili en önemli husus Bilgi Güvenliğinin ***üst yönetim*** sorumluluğunda yürütülecek bir faaliyet olduğudur. **Bilgi Güvenliği Politikaları Yönergesi gereği;** Bakanlık Merkez, Bağlı Kuruluşlar ve İl Sağlık Müdürlükleri (İSM'ler) bünyesinde, bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek üzere bilgi güvenliği alt komisyonlarının kurulması ve bilgi güvenliği yetkililerinin görevlendirilmesi gerekmektedir. Söz konusu komisyon ve bilgi güvenliği yetkilisi olarak görevlendirilen kişilerin görevlerini layıkıyla yapabilmesi için bağlı oldukları kurumların ***en üst düzey yöneticileri*** tarafından kuvvetli bir şekilde desteklenmesi gerekmektedir.

BAŞARILI OLMAK İÇİN ;

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımıza Bilgi Güvenliği Yönetim Sistemi Politikamızda yer verilmektedir.

Bilgi Güvenliği Mevzuatı

- Anayasa,
- 5237 sayılı Türk Ceza Kanunu,
- 4721 sayılı Türk Medeni Kanun,
- 3359 sayılı Sağlık Hizmetleri Temel Kanunu,
- 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun,
- 5258 sayılı Aile Hekimliği Pilot Uygulaması Hakkında Kanun,
- 663 sayılı Kanun Hükmünde Kararname,
- 5070 sayılı Elektronik İmza Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun",

Bilgi Güvenliği Mevzuatı

- 26687 sayılı “İnternet **Toplu Kullanım Sağlayıcıları** Hakkında Yönetmelik,
- 26716 sayılı “İnternet Ortamında Yapılan **Yayınların Düzenlenmesi**ne Dair Usul ve Esaslar Hakkında Yönetmelik”,
- 26680 sayılı “Telekomünikasyon Kurumu Tarafından **Erişim Sağlayıcılar**a ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”,
- Sağlık Bakanlığı ve Bağlı Kuruluşlarının **Elektronik Belge Yönetimi Sistemi** Uygulama Yönergesi,
- Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi.
- 03.09.2018 tarihli ve 67523305-719-E.4321 sayılı yazısı ile Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzu son güncel hali yürürlüğe girmiştir.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu Çerçevesinden

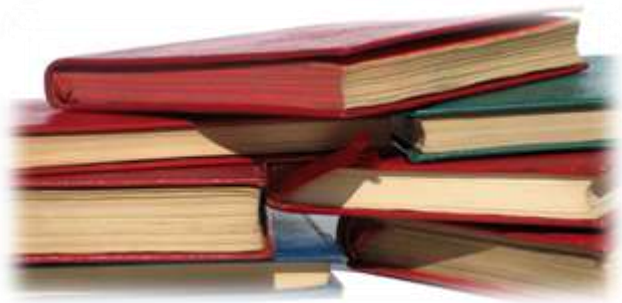
YÜRÜRLÜKTE OLAN KANUN VE YÖNETMELİKLER

Türkiye Cumhuriyeti Anayasası:

MADDE 20:

(Ek fıkra: 12/9/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

https://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf



5237 sayılı Türk Ceza Kanunu:

ONUNCU BÖLÜM – Bilişim Alanında Suçlar

<u>Bilişim sistemine girme:</u>

MADDE 243

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme:

MADDE 244. – (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) *Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır*.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur.

Veri Güvenliği Rehberi;

6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) uyarınca kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla veri sorumlularının alması gereken teknik ve idari tedbirlere ilişkin başlıca yöntemleri ayrı ayrı bölümler halinde açıklamaktadır.

6698 Sayılı Kanunun 12 nci maddesinin birinci fıkrasında;

Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” hükmü yer almaktadır.

Bu kapsamda, kişisel verilerin işlenmesi sürecinde veri sorumlularının alması gereken teknik ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla Kişisel Verileri Koruma Kurulu (“Kurul”) tarafından Kişisel Veri Güvenliği Rehberi (“Rehber”) hazırlanmıştır.

Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir.

Riskler belirlenirken;

- Kişisel verilerin özel nitelikli kişisel veri olup olmadığı,

- Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği,

- Güvenlik söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır.

İDARİ TEDBİRLER

Kişisel Veri İşleme Envanteri Hazırlanması
Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında)
Gizlilik Taahhütnameleri
Kurum İçi Periyodik ve/veya Rastgele Denetimler
Risk Analizleri
İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)
Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.)
Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

TEKNİK TEDBİRLER

Yetki Matrisi
Yetki Kontrol
Erişim Logları
Kullanıcı Hesap Yönetimi
Ağ Güvenliği
Uygulama Güvenliği
Şifreleme
Sızma Testi
Saldırı Tespit ve Önleme Sistemleri
Log Kayıtları
Veri Maskeleme
Veri Kaybı Önleme Yazılımları
Yedekleme
Güvenlik Duvarları
Güncel Anti-Virüs Sistemleri
Silme, Yok Etme veya Anonim Hale Getirme
Anahtar Yönetimi

A.BİLGİ GÜVENLİĞİ

Bilgi Güvenliği Organizasyonu

A.1.2.1. Genel Müdürlük tarafından, bilgi güvenliğinin iç organizasyonunun sağlanması için bilgi güvenliği konusunda uzmanlaşmış, bilgi sistemlerinin kapsamı göz önüne alınarak yeterli sayıda personelden oluşan, teknik, idari ve hukuki süreçlerde çalışmalarda bulunmak üzere "Bilgi Güvenliği Yönetim Komisyonu" oluşturulur.

A.1.2.2. Komisyona bağlı olarak çalışmak üzere bilgi güvenliğinin farklı alt alanlarında "çalışma grupları" teşkil edilir. Çalışma gruplarının oluşturulurken teknik, hukuki ve idari disiplinlerden personel bulunmalıdır.

A.1.2.3. Komisyonun Görevleri;

• Bilgi güvenliği politika ve stratejilerini belirler, gerektiğinde Bilgi Güvenliği Politikaları Yönergesine bağlı olarak çalışma grupları tarafından 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.

A.1.2.4. Bakanlık Merkez, bağlı kuruluşlar ve taşra teşkilatları kurumları bünyesinde, bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek üzere “Bilgi Güvenliği Yetkilisi ” görevlendirilir.

Bakanlık Merkez, bağlı kuruluşlar ve taşra teşkilatları üst yönetimleri hangi seviyede ve hangi alt kuruluşlarında “Bilgi Güvenliği Yetkilisi” görevlendireceklerine kurum bilgi sistemleri kapsamı, etki alanı, personel sayısı gibi kriterleri göz önüne alarak, ölçek yaklaşımı çerçevesinde karar verirler ve görevlendirecekleri Bilgi Güvenliği Yetkilisinin sorumluluk kapsamını belirlerler.

A.1.2.5. Bilgi Güvenliği Yetkilisinin ana işlevi; bulunduğu kurumdaki bilgi güvenliği faaliyetlerini Genel Müdürlük ile koordineli bir şekilde yürütmektir. Bilgi Güvenliği Yetkilisi olarak görevlendirilen personel Genel Müdürlük tarafından ana ilke ve politikalar konusunda eğitilir ve yönlendirilir.

B. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

VARLIKLARIN BELİRLENMESİ

- Bilgi,
- Donanım (kişisel bilgisayarlar, yazıcılar, sunucular),
- Yazılım (işletim sistemleri, geliştirilen uygulamalar, ofis programları),
- Haberleşme cihazları (telefonlar, hatlar, kablolar, modemler, anahtarlama cihazları),
- Dokümanlar(stratejik toplantıların tutanakları, sözleşmeler vb.),
- Üretilen mallar,
- Servisler,
- Personel,
- Kurumun prestiji / imajı.

Varlıkların belirlenmesinde kullanılabilecek bazı bilgi toplama teknikleri mevcuttur.

Tehditlerin Belirlenmesi

- Doğal tehditler
- Çevresel tehditler
- İnsan kaynaklı tehditler

Tehdit	Tehdidin Kaynağı
Deprem	D
Sel	D
Fırtına	D
Yıldırım	D
Endüstriyel bilgi sızması	B,K
Bombalama ve silahlı saldırı	B
Yangın	B,K
Güç kesintisi	B,K,Ç
Su kesintisi	B,K,Ç
Havalandırma sisteminin arızalanması	B,K,Ç
Donanım arızaları	K
Güç dalgalanmaları	K,Ç
Tozlanma	Ç
Elektrostatik boşalma	Ç
Hırsızlık	B
Saklama ortamlarının izinsiz kullanılması	B,K
Saklama ortamlarının eskiyip kullanılmaz duruma gelmesi	K
Personel hataları	K
Bakım hataları/eksiklikleri	K
Yazılım hataları	B,K
Lisanssız yazılım kullanımı	B,K
Yazılımların yetkisiz kullanılması	B,K
Kullanıcı kimlik bilgilerinin çalınması	B,K
Zararlı yazılımlar	B,K
Yetkisiz kişilerin ağa erişimi	B
Ağ cihazlarının arızalanması	K
Hat kapasitelerinin yetersiz kalması	B,K
Ağ trafiğinin dinlenmesi	B
İletim hatlarının hasar görmesi	B,K
İletişimin dinlenmesi	B
Mesajların yanlış yönlendirilmesi	K
Mesajların yetkisiz kişilere yönlendirilmesi	B
İnkar etme	B
Kaynakların yanlış kullanımı	K
Kullanıcı hataları	K
Personel yetersizliği	K

B: İnsan kaynaklı ve bilerek
K: İnsan kaynaklı ve kazayla
D: Doğal
Ç:Çevresel

AÇIKLARIN BELİRLENMESİ

Açıklık, sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır. Açıklıklar tek başlarına tehlike oluşturmazlar ve gerçekleşmeleri için bir tehdidin mevcut olması gerekir. Açıklık değerlendirmesi, tehditler tarafından gerçekleştirilebilecek açıklıkları ve bu açıklıkların ne kadar kolay gerçekleştirilebileceğini ele alır. Açıklıkların belirlenmesinde anket, birebir görüşme, dokümantasyon ve otomatik tarama araçları gibi yöntemler kullanılabilir.

OLASILIK DEĞERLENDİRMESİ

OLASILIK SEVİYESİ	OLASILIK SEVİYESİ
Yüksek	Tehdit kaynağı çok kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesini engelleyecek kontroller bulunmamaktadır veya etkisizdir.
Orta	Tehdit kaynağı kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesine engel olacak kontroller mevcuttur.
Düşük	Tehdit kaynağı daha az kabiliyetli ve motivasyonu daha düşüktür, açıklığın gerçekleşmesini engelleyecek veya çok zorlaştıracak kontroller mevcuttur.

ETKİ ANALİZİ

Etki Derecesi	Etki tanımı
YÜKSEK	Açıklığın gerçekleşmesi durumunda: Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir ve mali zarar çok büyük olur. Kurumun çıkarları, misyonu ve prestiji büyük zarar görebilir veya etkilenebilir. İnsan hayatı kaybı veya ciddi yaralanmalar gerçekleşebilir.
ORTA	Açıklığın gerçekleşmesi durumunda: Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrar. Kurumun çıkarları, misyonu ve prestiji zarar görebilir veya etkilenebilir. Yaralanmalar gerçekleşebilir.
DÜŞÜK	Açıklığın gerçekleşmesi durumunda: Kurumun bazı varlıkları etkilenir Kurumun çıkarları, misyonu ve prestiji etkilenebilir.

RİSK DERECELENDİRMESİ

Bu adımın amacı, varlıkları tehdit eden risklere değerler atayıp onları derecelendirmektir. Uygun kontrollerin seçilmesi burada belirlenen risklere ve seviyelere göre yapılır. Risk bir tehdidin bir açıklığı gerçekleme olasılığının, açıklığın ne kadar kolay gerçekleştirilebildiğinin ve mevcut veya planlanan kontrollerin yeterliliğinin bir fonksiyonudur. Yani kısaca olasılık değerlendirmesinde ve etki analizinde belirlenen değerlere bağlıdır. Risklerin ölçülebilmesi için risk sınıflandırma matrisi oluşturulmalıdır ve bu sınıflandırma için tanımlamalar yapılmalıdır.

C. POLİTİKALAR

- C.1 İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ
- C.2 FİZİKSEL VE ÇEVRESEL GÜVENLİK
- C.3 EKİPMAN GÜVENLİĞİ
- C.4 İŞLETİM SİSTEMLERİ VE SON KULLANICI GÜVENLİĞİ
- C.5 PAROLA GÜVENLİĞİ
- C.6 KRİPTOLAMA YÖNETİMİ
- C.7 İNTERNET VE ELEKTRONİK POSTA GÜVENLİĞİ
- C.8 SUNUCU VE SİSTEM GÜVENLİĞİ
- C.9 AĞ CİHAZLARI GÜVENLİĞİ
- C.10 MAL VE HİZMET ALIMLARI GÜVENLİĞİ
- C.11 UYGULAMA YAZILIMLARI GÜVENLİK YÖNETİMİ
- C.12 GÜVENLİK YAZILIM VE DONANIMLARI YÖNETİMİ
- C.13 BİLGİ GÜVENLİĞİ TEKNOLOJİLERİ GÜVENLİĞİ
- C.14 BULUT TEKNOLOJİLERİ GÜVENLİĞİ
- C.15 MOBİL CİHAZLAR GÜVENLİĞİ
- C.16 İLETİŞİM VE İŞLETİM GÜVENLİĞİ
- C.17 KULLANICI HESABI AÇMA, KAPATMA YÖNETİMİ
- C.18 ERİŞİM YÖNETİMİ VE ERİŞİM KAYDI TUTULMASI
- C.19 UZAKTAN ERİŞİM YÖNETİMİ
- C.20 ACİL ERİŞİM YETKİLENDİRME YÖNETİMİ
- C.21 VERİ MERKEZİ STANDARTLARI VE YÖNETİMİ
- C.22 VERİ TABANI GÜVENLİĞİ
- C.23 KAYDEDİLEBİLİR TAŞINIR MATERYALLER GÜVENLİĞİ
- C.24 BİLGİ SİSTEMLERİ EDİNİM GELİŞTİRME VE BAKIMI
- C.25 YEDEKLEME VE İŞ SÜREKLİLİĞİ YÖNETİMİ
- C.26 BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ
- C.27 BİLGİ GÜVENLİĞİ TEKNİK VE FARKINDALIK EĞİTİMLERİ
- C.28 DEĞİŞİM YÖNETİMİ
- C.29 İHLAL BİLDİRİM VE YÖNETİMİ
- C.30 BİLGİ GÜVENLİĞİ İZLEME VE DENETLEME YÖNETİMİ
- C.31 BİLGİ GÜVENLİĞİ TESTLERİ
- C.32 ACİL DURUM YÖNETİMİ
- C.33 BİLGİ GÜVENLİĞİ ULAŞTIRMA GÜVENLİĞİ YÖNETİMİ
- C.34 SOSYAL MÜHENDİSLİK ZAAFİYETLERİ
- C.35 SOSYAL MEDYA GÜVENLİĞİ
- C.36 SİSTEM AKREDİTASYONU
- C.37 MEDİKAL CİHAZLAR GÜVENLİĞİ

C.1 İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ

C.1.1 Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.

C.1.2 Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.

C.1.3 ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.

C.1.4 Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.

C.1.5 İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kağıt kesme makinasında imha edilmelidir.

C.1.6 Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

C.1.7 Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.

C.1.8 Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

C.1.9 Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

BİLGİ İŞLEM BİRİMİ

ORYANTASYON FORMU

AD-SOYAD	
UNVAN	
SİCİL NO	
Kadro yeri	
Mesleğe başlama tarihi	
GÖREVE BAŞLAMA TARİHİ	
ORYANTASYON TARİHİ	

TAMAMLANAN İŞLEMLER	EVET	HAYIR
Kurum organizasyon yapısının tanıtımı yapıldı.		
Hiyerarşi ve hiyerarşiye uygun iletişim hakkında bilgi verildi.		
Sağlık müdürlüğü binaları ve çalışılacak binanın tanıtımı yapıldı.		
Mesai saatleri ve molalar hakkında hatırlatma yapıldı.		
Birim görev tanımları yapıldı.		
Birim görev dağılımları hakkında bilgi verildi.		
Kişinin iş ve görev tanımı hakkında bilgi verildi.		
Ekip arkadaşları hakkında bilgilendirme yapıldı.		
Özlük hakları hakkında genel bilgi verildi.		
İzin – rapor konusunda bilgilendirme yapıldı.		
Kişinin birime başlayışı personel başkanlığından birimimize bildirildi.		
Başlayış yazısı yazıldı.		
Maaş-ödeme yazışmaları yapıldı		
Kimlik kartı talebi yapıldı.		
Kişisel veri güvenliği hakkında bilgi verildi.		
Bilgi güvenliği talimatnamesinin okundu, imzalandı.		
Kişisel parola ve yetki tanımlanmaları yapıldı		
Zimmet bilgisi güncellendi.		
ÇKYS ve PBS ye görevlendirmenin işlenip işlenmediği kontrol edildi.		

ORYANTASYON EĞİTİMİ ALAN İMZA	
ORYANTASYON EĞİTİMİ VEREN AD SOYAD İMZA	
BİRİM SORUMLUSU ONAY	

- C.2 FİZİKSEL VE ÇEVRESEL GÜVENLİK
  - Giriş
  - C.2.1 Fiziksel Güvenlik Sınırı
  - C.2.2 Fiziksel Giriş Kontrolleri
  - C.2.3 Ofislerin ve Odaların Güvenliğinin Sağlanması
  - C.2.4 Harici ve Çevresel Tehditlerden Korunma
  - C.2.5 Güvenli Alanlarda Çalışma
  - C.2.6

GİRİŞ

Fiziksel ve çevresel güvenlik, işyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.
Geçmiş zamanlarda önemli bilgiler, taşlara kazınarak daha sonra da kâğıtlara yazılarak fiziksel ortamlarda saklanmış, duvarlarla, kale hendekleriyle ve başlarına dikilen nöbetçilerle koruma altına alınmıştır. Çoğu zaman fiziksel koruma yeterli kalmamış ve bilgilerin çalınması ve başka kişilerin eline geçmesi engellenememiştir. Bu durum, verileri korumak için fiziksel güvenliğin tek başına yeterli olmadığını göstermektedir.
Günümüzde de fiziksel güvenlik önemini korumakta ve bu konuyla ilgili gerekli çalışmalar yapılmaktadır. Örneğin, bina etrafına yüksek duvarlar ya da demirler yapılması, bina girişinde özel güvenlik ekiplerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesi ya da bu odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler kullanılmaktadır.

C.2.1 Fiziksel Güvenlik Sınırı

C.2.1.1. Bilgi işleme servisini korumak amacıyla herhangi bir fiziksel sınır güvenliği tesisi kurulmuş olmalıdır. (Kart kontrollü giriş, duvarlar, insanlı nizamiye)

C.2.1.2. Fiziksel sınır güvenliği, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre oluşturulmalıdır.

C.2.2 Fiziksel Giriş Kontrolleri

C.2.2.1. Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurulmalıdır.

C.2.2.2. Kapsam ve prosedürü idarelerce belirlenmek suretiyle ziyaretçilerin giriş ve çıkış zamanları kaydedilmelidir.

C.2.2.3. Hassas bilgilerin bulunduğu alanlar (kimlik doğrulama kartı ve PIN koruması gibi yöntemlerle) yetkisiz erişime kapatılmalıdır.

C.2.2.4. Kapsam ve prosedürü idarelerce belirlenmek suretiyle tüm personel ve ziyaretçiler güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartlarını devamlı takmalıdır.

C.2.2.5. Güvenli alanlara erişim hakları düzenli olarak gözden geçiriliyor olmalıdır.

C.2.3 Ofislerin ve Odaların Güvenliğinin Sağlanması

C.2.3.1. Ofisler ve odalarla ilgili fiziksel güvenlik önlemleri alınmalıdır.

C.2.3.2. Personel güvenliği ve sağlığı ile ilgili yönetmelikler uygulanmalıdır.

C.2.3.3. Kritik tesisler kolayca ulaşılamayacak yerlere kurulmuş olmalıdır.

C.2.3.4. Binada bilgi işlem faaliyetlerinin yürütüldüğüne dair işaret, tabela vb. bulunmamasına dikkat edilmelidir.

C.2.3.5. Bilgi işlem merkezlerinin konumunu içeren dâhili/harici telefon rehberleri halka kapalı olmalıdır.

C.2.4 Harici ve Çevresel Tehditlerden Korunma

C.2.4.1. Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karsı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.

C.2.4.2. Komşu tesislerden kaynaklanan potansiyel tehditler göz önünde bulundurulmalıdır.

C.2.4.3. Yedeklenmiş materyal ve yedek sistemler ana tesisten yeterince uzak bir yerde konuşlandırılmış olmalıdır.

C.2.5 Güvenli Alanlarda Çalışma

C.2.5.1. Güvenli çalışma alanlarındaki personel veya bu alanda yürütülmekte olan çeşitli faaliyetlerde bulunan personel ve üçüncü parti çalışanları için "ihtiyacı kadar bilme" prensibi uygulanmalıdır.

C.2.5.2. Kayıt cihazlarının güvenli alanlara sokulmasına engel olunmalıdır.

C.2.5.3. Kullanılmayan güvenli alanlar kilitleniyor ve düzenli olarak kontrol ediliyor olmalıdır.

C.2.5.4. Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir.

C.2.5.5. Güvenli bölgelere örneğin sistem odasına yapılan girişler kayıt altına alınmalıdır.

C.2.6

Bilgi işlem servisleri ile dağıtım ve yükleme alanları ve yetkisiz kişilerin tesislere girebileceği noktalar birbirinden izole edilmiş olmalıdır.

C.3 EKİPMAN GÜVENLİĞİ

- C.3.1
- C.3.2 Belli Başlı Temiz Masa Kuralları
- C.3.3 Ekipman Yerleşimi ve Koruması
- C.3.4 Destek Hizmetleri
- C.3.5 Kablolama Güvenliği
- C.3.6 Ekipman Bakımı

C.3 EKİPMAN GÜVENLİĞİ

C.3.1

Masalarda ya da çalışma ortamlarında korumasız bırakılmış bilgiler yetkisiz kişilerin erişimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle bütünlüğünün bozulmalarına ya da yok olmalarına sebep olabilir. Tüm bu veya daha fazla tehditleri yok edebilmek için aşağıda yer alan belli başlı temiz masa kurallarına ilişkin politikalar geliştirilmeli ve bu politikaların çalışanlar tarafından haberdar olunması sağlanmalıdır.

C.3.2 Belli Başlı Temiz Masa Kuralları

C.3.2.1. Hassas bilgiler içeren evraklar, bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir. Bu bilgi ve belgelerin kilitli yerlerde muhafaza edilmesi gerekmektedir.

C.3.2.2. Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir.

C.3.2.3. Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır.

C.3.2.4. Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yakma vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir.

C.3.2.5. Faks makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmamalıdır.

C.3.2.6. Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), PCler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

Bilgisayarınızı kullanırken

Bilgisayarınıza girerken şifrenin başkaları tarafından görülmemesi sağlanmalıdır.

Kullanıcı isminizi ve kullanıcı haklarınızı kullanarak başka bir kimsenin işlem yapmasına izin verilmemelidir.

Bilgisayar başından kalkarken ekran kilitlenmelidir. (Windows logo tuşu + L)
Şifre korumalı ekran koruyucusu ayarlanmalıdır.

C.3.3 Ekipman Yerleşimi ve Koruması

C.3.3.1. Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmalıdır.

C.3.3.2. Ekipman, gereksiz erişim asgari düzeye indirilecek şekilde yerleştirilmelidir.

C.3.3.3. Kritik veri içeren araçlar yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilmelidir.

C.3.3.4. Özel koruma gerektiren ekipman izole edilmiş olmalıdır.

C.3.3.5. Nem ve sıcaklık gibi parametreler izlenmelidir.

C.3.3.6. Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanmalıdır.

C.3.3.7. Paratoner kullanılmalıdır.

C.3.3.8. Bilgi işlem araçlarının yakınında yeme, içme ve sigara içme konularını düzenleyen kurallar olmalıdır.

C.3.4 Destek Hizmetleri

C.3.4.1. Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem dairesi için yeterli düzeyde olmalıdır.

C.3.4.2. Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmış olmalıdır.

C.3.4.3. Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır.

C.3.4.4. Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.

C.3.4.5. Acil durumlarda iletişimin kesilmemesi için servis sağlayıcıdan iki bağımsız hat alınmalıdır.

C.3.4.6. Kurum bu konuda yasal yükümlülüklerini yerine getirmelidir.

C.3.7 Kurum Dışındaki Ekipmanın Güvenliği

C.3.7.1. Kurum alanı dışında bilgi işleme için kullanılacak ekipman için yönetim tarafından yetkilendirme yapılıyor olmalıdır.

C.3.7.2. Tesis dışına çıkarılan ekipmanın başıboş bırakılmamasına, seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilmelidir.

C.3.7.3. Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulmalıdır.

C.3.7.4. Evden çalışma ile ilgili tedbirler alınmalıdır. Cihazların sigortaları, tesis dışında korumayı da kapsamalıdır.

C.3.7.5. Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenmelidir.

C.10 MAL VE HİZMET ALIMLARI GÜVENLİĞİ

C.10.1

Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir.

C.10.2

Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

- Bilgi güvenliği politikası,
- Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,
- Gerekli fiziki koruma için kontrol ve mekanizmalar,
- Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,
- Varlıklarda oluşan herhangi bir değişimin tespiti için

prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan

kayıp veya modifikasyon,
- Anlaşma sırasında, sonrasında ya da zaman içinde kabul

edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,
- Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,
- Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,
- Kullanıcı ve yönetici eğitimlerinin methodu, prosedürü ve güvenliği,
- Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,

• Uygun olduğu yerde personel transferi için hüküm,

• Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,

• Açık bir raporlama yapısı ve anlaşılan raporlama formatı,

• Değişim yönetimi sürecinin açıkça belirlenmesi,

• Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,

• İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,

• Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,

• Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,

• Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,

• Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,

• Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,

• Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,

• Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,

• Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,

• Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,

- Sorun çözümü için bir yükseltme sürecinin kurulması,
- Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik de dahil olmak üzere hizmet sürekliliği gerekleri,
- Anlaşmayla ilgili tarafların yükümlülükleri,
- Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak)
- Fikri mülkiyet hakları (IPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,
- Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri,
- Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,
- Taraflardan birinin anlaşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır.
- Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların yeniden müzakere edilmesi,
- Varlık listeleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

C.10.3 Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar önemli ölçüde değişebilir. Bu nedenle; anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde yapılmalıdır. Gerektiğinde güvenlik yönetim planındaki gerekli kontroller ve prosedürler genişletilebilir.

C.10.4 Bilgi güvenliği yönetimi dış kaynaklı ise anlaşmalarda üçüncü tarafın güvenlik garantisinin yeterliliğini nasıl ele alındığı anlaşmada belirtilmelidir. Risk değerlendirmede tanımlandığı gibi, risklerdeki değişiklikleri belirlemek ve başa çıkmak için güvenliğin nasıl adapte edileceği ve sürdürüleceği ele alınmalıdır.

C.10.5 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 feshedilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.

C.10.6 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.

C.10.7 Genellikle anlaşmaların esasları kuruluşlar tarafından geliştirilmiştir. Bazı durumlarda anlaşmaların üçüncü taraflarca geliştirilmesi ve kuruluşa empoze edilmesi durumu olabilir. Kuruluşlar, kendi yapılarına üçüncü taraflarca empoze edilecek anlaşmalarda kendi güvenliklerinin gereksiz yere etkilenmesini engeller

C.10.8 Gizlilik sözleşmeleri;

C.10.8.1. Gizlilik veya ifşa etmeme anlaşmaları yasal olarak uygulanabilir terimleri kullanarak gizli bilgileri korumanın gerekliliğini ele almalıdır. Gizlilik veya ifşa etmeme anlaşmaları için aşağıdaki unsurlar dikkate alınmalıdır:

- Korunacak bilginin bir tanımı (örneğin; gizli bilgileri),
- Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dahil olmak üzere anlaşma süresi,
- Anlaşma sona erdiğinde yapılması gereken eylemler,
- Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi (‘bilmesi gereken’ gibi),
- Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiği,
- Gizli bilgilerin kullanım izni ve bilgileri kullanmak için imza hakları,
- Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,
- Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesinin bildirimi ve raporlama prosesi,
- İade veya imha anlaşmasına bırakılacak bilgi için terimler,
- Bu anlaşmanın ihlali durumunda yapılması beklenen eylemler.

C.10.8.2. Bir kuruluşun güvenlik gereksinimlerine dayalı olarak, diğer unsurlarla bir gizlilik veya ifşa etmeme anlaşması gereklidir.

C.10.8.3. Gizlilik ve ifşa etmeme anlaşmaları uygulandığı yerin geçerli tüm yasa ve yönetmeliklerine uygun olmalıdır.

C.10.8.4. Gizlilik ve ifşa etmeme anlaşmaları için gerekler periyodik olarak veya gerekleri etkileyecek bir değişiklik olduğunda gözden geçirilmelidir.

C.10.8.5. Gizlilik ve ifşa etmeme anlaşmaları kurumsal bilgileri korumalı ve imzalayanın, bilginin korunmasından, kullanılmasından ve ifşa edilmesinden yetkili ve sorumlu olduğunu belirtmelidir.

C.10.8.6. Farklı koşullarda gizlilik ve ifşa etmeme anlaşmaları kuruluşun ihtiyaçları

doğrultusunda farklı şekillerde kullanılmalıdır.

C.15 MOBİL CİHAZLAR GÜVENLİĞİ

Giriş

Bilgiyi taşımanın kolay bir yolu laptop ve akıllı telefonlar gibi mobil cihazlardır. Bu cihazlarda bulunan hassas bilgiler ve erişim yetkileri de düşünüldüğünde mobil cihazlarda güvenliğin dikkat edilmesi gereken bir konu olduğu anlaşılmaktadır.

C.15.1

Mobil cihazlara erişimde mutlaka parola kullanılmalıdır.

C.15.2

Mobil cihazınızda ne tür bilgiler sakladığınızın farkında olun, hassas ve gizli bilgileri mümkün olduğunca mobil cihazınızda bulundurmayınız.

C.15.3

Verilerinizin yedeklerini alın ve güncel bir kopyasını farklı bir yerde saklayınız.

C.15.4

Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

C.17 KULLANICI HESABI AÇMA, KAPATMA YÖNETİMİ

C.17.1 Kullanıcı hesabı tanımlanması için 2 yöntem uygulanır.

C.17.1.1. Bağlı bulunulan kurumdan resmi yazı yazılması şeklinde yapılmalıdır.

C.17.1.2. Bağlı bulunulan kurum yetkilisi tarafından @saglik.gov.tr uzantılı bir resmi e-posta adresi ile talep ettikleri yeni kullanıcılar için hazırlanan formu doldurarak eposta@saglik.gov.tr resmi e-posta adresine taleplerini göndermeleri şeklinde yapılmalıdır. Kullanıcı talebine göre yetki verilmesi durumunda ayrıca taahhütname istenilebilir.

C.17.2 Yeni kullanıcı oluşturulması taleplerinde, kişinin Başbakanlık DTVT sistemine uygun olarak konumlandırılacağı Kurum birimi, ekleneceği yetki grupları, görev tipine göre istenir. 657, 4A, 4B dışındaki personel için çalışma süre aralığının belirtilmesi gereklidir.

C.17.3 Kullanıcı hesabının dondurulması, kapatılması kullanıcının bağlı olduğu personel işleri veya bilgi işlem tarafından C.17.1.1 ve C.17.1.2 maddelerindeki erişim kanalları ile bildirilmelidir.

C.17.4 Kullanıcı hesabı kapatma talebi gelmesine istinaden dondurulur ve dondurulmuş hesaplar klasöründe bir sene süresince yasal takip ihtiyaçlarına binaen saklanır ve bir sene sonunda silinmelidir.

C.18 ERİŞİM YÖNETİMİ VE ERİŞİM KAYDI TUTULMASI

Giriş

Veri tabanlarına erişen kullanıcıların yapmış oldukları işlemler loglanmalı, gerektiğinde erişim yetkilisinin kayıt silme logları da listelenebilir olmalıdır.

C.18.1. Erişim Yönetimi

C.18.1.1. Kurumun erişim sağlanacak sunucularına admin/root yetkili yönetici kullanıcılar, sudo ve runas yetkili kısıtlı yönetici kullanıcılar ve dış dünyadan erişen, uygulamayı kullanan kullanıcılardan oluşmaktadır.

C.18.1.2. Bakanlık sunucularına erişim için IP/SEC ya da SSL VPN kullanılmalıdır.

Mümkünse kullanıcıların erişimi için SSL ve VPN tercih edilmelidir. Güvenlik Birimi tarafından sağlanmalıdır.

C.18.1.3. Sunuculara kullanıcı erişimi için SSH, RDP gibi protokollerle sunucu yönetimi için belirli portlar erişim verilmelidir.

C.18.1.4. Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.

C.18.1.5. Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir. Parola yönetimi bakanlık bilgi güvenliği kılavuzundaki parola yönetim politikaları ile yürütülmelidir.

C.18.1.6. Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, ssh-key) ile yapılmalıdır.

C.18.1.7. Kullanıcıların sunucu yönetim için sağlanan erişimde sudo, runas gibi erişim kısıtlı erişim yetkileri tanımlanmalıdır.

C.18.1.8. Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir. Güvenlik Birimi tarafından bu işlem sağlanmalıdır.

C.18.1.9. Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri, sistem gurubuna teslim edilmelidir. Sistem birimi nezaretinde ve tarafından yürütülmelidir.

C.18.1.10. Sunucu servislerinin yönetim işlemleri merkezi kullanıcı yönetimi ve kısıtlı erişim yetkileriyle kullanıcılara sağlanmalıdır.

C.18.1.11. Kurumun yedekleme sistemlerine sadece memur ya da danışman yetkili kişi erişim yapmaktadır. Firmaların yapacakları tüm işlemler sistem birimi nezaretinde yürütülmelidir.

C.18.2 Kayıt Tutulması (Log Tutulması)

C.18.2.1. Kurumun güvenlik cihazlarına ait loglar güvenlik birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.

C.18.2.2. Kurumun veri tabanlarına ait loglar veri tabanları birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.

C.18.2.3. Kurumun network cihazlarına ait loglar network birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.

C.18.2.4. Tüm sunuculara ve servislere sağlanan tüm yönetici erişimleri uzak ve merkezi bir kayıt sunucusuna gönderilmelidir.

C.18.2.5. Merkezi kayıt sunucusu üzerinde yapılan analizler sonucunda başarısız erişimler raporlanmalıdır.

C.18.2.6. Merkezi kayıt sunucusu üzerinde alınan başarısız erişim istekleri uyarı olarak yetkili Birimlere gönderilmelidir.

C.18.2.7. Merkezi kayıt sunucusu üzerindeki başarılı girişler de istatiksel veriler halinde raporlanabilmelidir.

C.18.2.8. Merkezi kayıt sunucusu üzerindeki kayıt verileri belirli tarih aralığında tutulmalı ve istenildiğinde raporlanabilir olmalıdır.

C.18.2.9. Merkezi kayıt sunucusu kayıtlar üzerinde yaptığı analizler doğrultusunda saldırı ve normal olmayan durumları tespit edip, uyarı gönderebilmelidir.

C.23 KAYDEDİLEBİLİR TAŞINIR MATERYALLER GÜVENLİĞİ

Giriş

USB flash diskler ve harici hddler; yüksek veri kapasiteleri, boyutları, taşınabilirlikleri ve farklı sistemlerde sorunsuzca çalışabilmeleri ile yanımızdan hiçbir zaman ayırmadığımız temel ihtiyaçlarımızdandır. Hemen hemen her sistemde çalıştırılabiliyor olmaları nedeniyle de bilgisayarlar arası veri alışverişimizi USB diskler ve harici hddler yardımıyla yapıyoruz.

USB disklerimizi onlarca farklı bilgisayarda kullanıyor, yine bilgisayarımıza onlarca farklı diskin takılmasına izin veriyoruz. Aslında USB diskleri tehlikeli kılan da bu çok da denetimli olmayan taşınabilirlikleri. Taşınabilir medya üzerinden bilgisayara giren zararlı yazılımlar başta bilgi sızdırma, uzaktan komut koşturma ve servis dışı bırakma olmak üzere birçok güvenlik zafiyetine neden olabilmektedir.

C.26 BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ

C.26.1 Bakanlık ve Bağlı Kuruluşlar kendi bünyelerinde oluşturacakları arşivden sorumludur. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.

C.26.2 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.

C.26.3 Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.

C.26.4 İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.

C.26.5 Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.

C.26.6 Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.

C.26.7 Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.

C.26.8 Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.

C.26.9 Hacimsel küçültme işlemi için parçalanmalıdır.

C.26.10 Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.

C.26.11 Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

C.28 DEĞİŞİM YÖNETİMİ

C.28.1 Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.

C.28.2 Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.

C.28.3 Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve dokümante edilmelidir.

C.28.4 Değişiklikler gerçekleştirilmeden önce kurumun ilgili biriminden onay alınmalıdır.

C.28.5 Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.

C.28.6 Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.

C.28.7 Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.

C.28.8 Teknoloji değişikliklerinin kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmeli ve dokümante edilmelidir.

C.28.9 Değişiklik yönetimini işletmek için bir talep yönetim sistemi kurmak ve işletmek önemlidir. Talebin nasıl alınacağı ve değerlendirileceği gibi esaslar tanımlanmalıdır.

C.28.10 Değişiklik onayının, "hangi kontroller ne şekilde yapıldıktan sonra verileceği"

tanımlanmalıdır.

C.28.11 Değişiklik öncesi test süreci tanımlanmalıdır.

C.28.12 Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler

tanımlanmalıdır.

C.29 İHLAL BİLDİRİM VE YÖNETİMİ

C.29.1 Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.

C.29.2 Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

C.29.3 Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.

C.29.4 Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.

C.29.5 İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

C.29.6 Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.

C.29.7 Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.

C.29.8 Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınır.

C.29.9 Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.

C.29.10 İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.

C.29.11 Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.

C.29.12 Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.

C.29.13 Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;

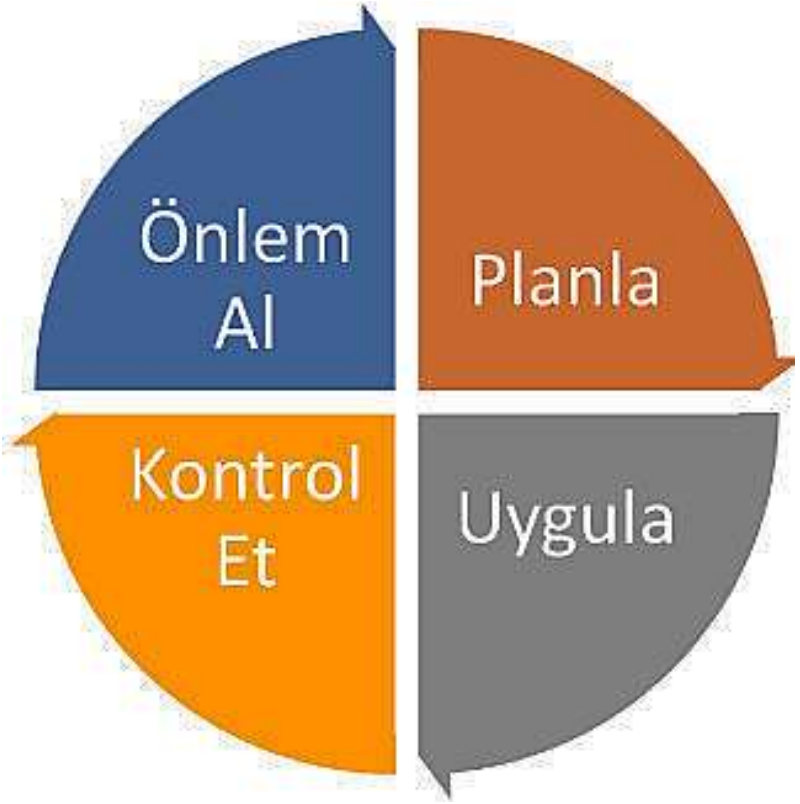
- Kanıtın mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,
- Kanıtın niteliği ve tamlığını gösteren ağırlığı.

C.29.14 Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

- Uyarma,
- Kınama,
- Para cezası,
- Sözleşme feshi.

BİLGİ GÜVENLİĞİ İHLAL BİLDİRİMLERİ

Bilgi güvenliği ihlal bildirimleri anında Bilgi Güvenliği Yetkilisine bildirilir. Bilgi Güvenliği Yetkilisi, Kurumu için Kılavuz çerçevesinde “Bilgi Güvenliği Planı” yapar ve bu Plan görev yaptığı kurum idaresince onaylanır. Bilgi güvenliği yönetimi, başlangıç ve bitiş tarihleri olan bir proje gibi görülmemelidir. Sürekli devam eden bir gelişim süreci olarak düşünülmelidir. PUKÖ modelinde gösterildiği gibi (Planla – Uygula – Kontrol et – Önlem al) faaliyetleri bir döngü içinde durmaksızın sürekli devam etmelidir.



PUKÖ modeli özet olarak ne yapılacağına karar verilmesi, kararların gerçekleştirilmesi, çalıştığının kontrol edilmesi hedefine uygun çalışmayan kontroller için önlemlerin alınmasıdır. BGYS kurulumu PUKÖ modelinin ilk adımını (Planla) teşkil etmektedir. Yerleşik bir sistemden bahsedebilmek için diğer adımların da uygulanması ve bunların bir döngü içinde yaşaması gerekir.

Bilgi Güvenliği İhlal Bildirimi için İl Sağlık Müdürlüğü Web Sitesini ziyaret edebilirsiniz.

http://www.ism.gov.tr/BGIhlalBildirimi.aspx

Yılda En Az Bir Kez Bilgi Güvenliği Eğitimi Alan Personel Oranı			
GK:	Yayın Tarihi:	Revizyon Tarihi:	Revizyon No:

Sözleşme Pozisyonu	Destek Hizmetleri Başkanı
Performans Kriteri	Sağlık Tesislerinde Bilgi Güvenliğine Yönelik Çalışmaların Yürütülmesini Sağlamak
Gösterge Kodu	TT.DH.3.1
Gösterge Adı	Yılda En Az Bir Kez Bilgi Güvenliği Eğitimi Alan Personel Oranı
Amacı	Yılda en az bir kez tüm personele bilgi güvenliği eğitimi verilmesini sağlamak
Hesaplama Parametreleri	A: Bilgi Güvenliği Eğitimi Alan Personel Sayısı B: Toplam Personel Sayısı C: Yılda En Az Bir Kez Bilgi Güvenliği Eğitimi Alan Personel Oranı
Hesaplama Formülü	C = (A/B)*100 C ≥ %95 ise GP=5 %90 ≤ C < %95 ise GP=3 %85 ≤ C < %90 ise GP=1 C < %85 ise GP=0
Gösterge Hedefi	Yılda En Az Bir Kez Bilgi Güvenliği Eğitimi Alan Personel Oranının %95 ve üzerinde olmasını sağlamak
Gösterge Puanı	5
Açıklama	Bu gösterge verisi Sağlık Bilgi Sistemleri Genel Müdürlüğü'nce temin edilecektir.
Veri Kaynağı	Bilgi Güvenliği Daire Başkanlığı / İSM
Veri Toplama Periyodu	1 Yıl
Veri Analiz Periyodu	1 Yıl

İl Genelindeki Tüm Kurumların Bilgi Güvenliği Politikalarına Uyum Oranı			
GK:	Yayın Tarihi:	Revizyon Tarihi:	Revizyon No:

Sözleşme Pozisyonu	Destek Hizmetleri Başkanı
Performans Kriteri	Sağlık Tesislerinde Bilgi Güvenliğine Yönelik Çalışmaların Yürütülmesini Sağlamak
Gösterge Kodu	TT.DH.3.2
Gösterge Adı	İl Genelindeki Tüm Kurumların Bilgi Güvenliği Politikalarına Uyum Oranı
Amacı	Sağlık bilgilerinin mahremiyete, standart ve algoritmalara uygun olarak zamanında toplanmasını sağlamak.
Hesaplama Parametreleri	A: Uyum Raporlaması Yapılan Kurum Sayısı B: Toplam Kurum Sayısı C: İl Genelindeki Tüm Kurumların Bilgi Güvenliği Politikalarına Uyum Oranı
Hesaplama Formülü	C = (A/B)*100 C ≥ %95 ise GP=5 %90 ≤ C < %95 ise GP=3 %85 ≤ C < %90 ise GP=1 C < %85 ise GP=0
Gösterge Hedefi	İl Genelindeki Tüm Kurumların Bilgi Güvenliği Politikalarına Uygun Olarak Raporlama Oranının %95 ve üzerinde olmasını sağlamak
Gösterge Puanı	5
Açıklama	Bu gösterge verisi Sağlık Bilgi Sistemleri Genel Müdürlüğü'nce temin edilecektir. İl genelindeki tüm kurumların SBSGM tarafından Bilgi Güvenliği Politikaları Kılavuzundan ilgili dönem için belirlenmiş olan başlıkların raporlanması dikkate alınacaktır.
Veri Kaynağı	Bilgi Güvenliği Daire Başkanlığı / İSM
Veri Toplama Periyodu	1 Yıl
Veri Analiz Periyodu	1 Yıl

İL GENELİNDEKİ KURUMLARIN BİLGİ GÜVENLİĞİ POLİTİKALARINA UYUM ORANININ HESAPLANMASINDA KULLANILACAK BAŞLIKLAR

S.No	Değerlendirme Yapılacak Başlık	Değerlendirilecek Başlık Kapsamında Kurumlar Tarafından Yapılması Beklenen Faaliyetler	Değerlendirilecek Başlık Kapsamında Hastane/İSM tarafından İSM/SBSGM'ye Gönderilecek Dokümanlar
1	Kurumsal BGYS Politikalarının Oluşturulması ve Uygulanması	1. Kurumun bilgi güvenliği amaç, kapsam, hedef, organizasyon gibi konu başlıklarının yer aldığı bir bilgi güvenliği politikası oluşturulması ve bunun yazılı bir doküman halinde yayımlanması 2. Hazırlanan politika dokümanının tüm kurum personeline tebliğ edilmesi/duyurulması	1. Kurumun Bilgi Güvenliği Yönetim Sistemi Politikası 2. Politikanın personele tebliğ edildiğine dair deliller (resmi yazı sureti, web sitesi erişim kayıtları, tebliğ belgesi, e-posta kayıtları vb.)
2	Bilgi Güvenliği Organizasyonu	1. Kurumun bilgi güvenliği politika ve stratejilerini belirlemek ve bu politikaların uygulanmasını sağlamak üzere bilgi güvenliği alt komisyonu oluşturulması 2. Siber olaylara müdahale ile ilgili faaliyetleri yürütmek üzere ilgi (ç) Kurumsal SOME Kurulum ve Yönetim Rehberinde belirtilen esaslar doğrultusunda Kurumsal SOME oluşturulması 3. Kurum Bilgi Güvenliği Yetkisi ve Kurumsal SOME Ekip Lideri görevlendirmesi yapılması 4. Bilgi Güvenliği Alt komisyonu toplantılarının yapılması, Bilgi Güvenliği Politikaları Kılavuzu gereği Alt Komisyon tarafından yürütülmesi gereken faaliyetlerin görüşülmesi, ilgili dokümanlara onay verilmesi, gerekli kararların alınması (Yukarıdaki hususların tamamının yapılmasından İSM'ler sorumlu olup Hastaneleri ilgilendiren kısımlar bir sonraki sütunda açıklanmıştır)	İSM'ler: 1. Bilgi Güvenliği Alt Komisyonu Görevlendirme Yazısı 2. Kurumsal SOME Görevlendirme Yazısı 3. Bilgi Güvenliği Yetkilisi ve Kurumsal SOME Ekip Lideri Görevlendirme Yazısı 4. Bir adet komisyon toplantı karar tutanağı Hastaneler: Bilgi güvenliği yetkilisi görevlendirmesi yapılmış ise konuyla ilgili görevlendirme yazısı Açıklama: Bilgi güvenliği politikaları yönergesi uyarınca hangi seviyede bilgi güvenliği yetkilisi ataması yapılacağı, İSM yetkisindedir. İSM tarafından yayınlanan İl Bilgi Güvenliği Yönetim Politikasında hastaneler (ve eşiti kurumlar) için bilgi güvenliği yetkilisi atanmayacağı, bu hizmetlerin ildeki

S.No	Değerlendirme Yapılacak Başlık	Değerlendirilecek Başlık Kapsamında Kurumlar Tarafından Yapılması Beklenen Faaliyetler	Değerlendirilecek Başlık Kapsamında Hastane/İSM tarafından İSM/SBSGM'ye Gönderilecek Dokümanlar
			Bilgi Güvenliği Yetkilisi tarafından yürütüleceği belirtilmiş ise, hastaneler bu maddeden değerlendirmeye tabi tutulmayacaktır.
3	Etki Alanı Kurulum ve Yönetimi	1. Kurumun bilgi sistemleri kullanıcı ve bilgisayarlarını yönetebilir ve denetlenebilir hale getirmek için etki alanı (DC) (veya benzeri bir yönetim yapısı) kurulması, tüm kullanıcı ve bilgisayarların etki alanına alınması 2. Etki alanı vasıtası ile tüm bilgisayar ve kullanıcıları kurumun bilgi güvenliği politikası, parola politikası ve ilgili diğer politika ve prosedürlerde belirtilen kurallara uymaya zorlayacak bir grup politikası (GPO) oluşturulması ve uygulanması	İSM'ler: 1. Etki alanı sunucusu ile ilgili bilgiler (Makine adı, IP adresi, etki alanı adı vb.) 2. Etki alanı OU yapısını gösteren ekran görüntüleri 3. Etki alanında uygulanan GPO'nun çıktısı Hastaneler: Yukarıdakilere ilave olarak kurum parola politikasının SBYS'lerde de uygulandığına dair ilgili uygulamadan alınacak ekran görüntüleri veya benzeri deliller Açıklama: 1. Yukarıdaki çıktılar kurumda Microsoft DC kullanıldığı varsayımı ile hazırlanmıştır. Kurumda Linux ve türevleri (Pardus vb.) kullanılıyorsa söz konusu işletim sistemi tarafından sağlanan kullanıcı yönetim yapısına ilişkin benzeri çıktılar gönderilecektir. 2. İlde bulunan tüm sağlık teşkillerinin etki alanı yönetimi İSM tarafından yapılıyor ise Hastaneler tarafından "Etki alanı sunucusu ile ilgili bilgiler" gönderilmeyecektir.

S.No	Değerlendirme Yapılacak Başlık	Değerlendirilecek Başlık Kapsamında Kurumlar Tarafından Yapılması Beklenen Faaliyetler	Değerlendirilecek Başlık Kapsamında Hastane/İSM tarafından İSM/SBSGM'ye Gönderilecek Dokümanlar
4	Erişim Kontrolü	1. Kılavuzun erişim kontrolü ile ilgili maddesine belirtilen şekilde kurumda kullanılan sistem ve uygulamaları kapsayacak şekilde kuruma özgü erişim kontrol politikası oluşturulması, politika dokümanında uygulama/sistemlere kullanıcıların (rollerin veya grupların) hangi yetkiler ile erişeceğini açıklayan detaylı bilgilere yer verilmesi 2. Kurum erişim kontrol politikası ile uyumlu olacak şekilde, kurum ağında yer alan kaynaklara (sunucu ve hizmetlere) uzaktan erişim için alınması gereken tedbirler ve uyulması gereken kuralları açıklayan bir prosedür hazırlanması.	1. Erişim kontrol politikası 2. Uzaktan erişim prosedürü
5	İnsan Kaynakları ve Son Kullanıcı Güvenliği	1. İşe başlama, görev değişikliği ve işten ayrılma süreçlerinde uygulanmak üzere kurum personelinin uyması gereken bir prosedürün hazırlanması 2. İşe başlama ve işten ayrılma formlarının oluşturulması 3. Devlet memuru/işçi statüsünde çalışan personele bilgi güvenliği farkındalık bildirgesinin tebliğ edilmesi 4. Yüklenici firmalar üzerinden çalışan personel ile personel gizlilik sözleşmesinin imzalanması	1. İşe başlama, görev değişikliği ve işten ayrılma süreçlerini tanımlayan prosedür 2. İşe başlama ve işten ayrılma süreci ve ilgili formlar 3. Kurum için özelleştirilmiş Personel Gizlilik Sözleşmesi ve Bilgi Güvenliği Farkındalık Bildirgesi 4. Bilgi güvenliği farkındalık bildirgesi ve kişisel gizlilik sözleşmesinin personele tebliğ edilmesine ilişkin kayıtlar (personel tarafından imzalan üç adet sözleşme/bildirge örneği)
6	Taşınabilir Ortam Yönetimi ve Ortamın Yok Edilmesi	1. Dizüstü bilgisayar, tablet, akıllı telefon, taşınabilir bellek, USB bellek, CD/DVD gibi taşınabilir ortamların kullanımında dikkat edilecek hususları açıklayan bir prosedür oluşturulması	1. Taşınabilir ortam yönetimi prosedürü 2. Bilgi saklama ortamları yok etme prosedürü

S.No	Değerlendirme Yapılacak Başlık	Değerlendirilecek Başlık Kapsamında Kurumlar Tarafından Yapılması Beklenen Faaliyetler	Değerlendirilecek Başlık Kapsamında Hastane/İSM tarafından İSM/SBSGM'ye Gönderilecek Dokümanlar
		2. Basılı ortamlar ve bilgi işlem cihazları da dahil her türlü ortamda saklanan bilgilerin silinmesi, anonim hale getirilmesi ve imha edilmesi ile ilgili hususları açıklayan bir prosedür oluşturulması	3. Bu çerçevede yapılan yok etme işlemlerine ilişkin kanıtlar (tutanak vb.)
7	Bilgi güvenliği İhlal Olayı Bildirim ve Yönetimi	1. Bilgi güvenliği ihlal olaylarının Bakanlık tarafından sunulun merkezi ihlal bildirim sistemine girilmesi hususunun, tüm çalışanlara resmi yazı, duyuru veya farkındalık eğitimi ile bildirilmesi 2. Yerel olarak işlem yapılarak ihlal bildirimleri doğrultusunda tedbirler alınması ve ihlal bildirim ve müdahale formlarının işlenmesi	1. Merkezi ihlal bildirim sisteminin kullanılacağına yönelik çalışanlara yapılan bildirim ile ilgili kanıtlar (resmi yazı vb.) 2. Yerel olarak işlem yapılan bildirimlere ait işlenmiş ihlal bildirim ve müdahale formları (üç adet)
8	Mal ve Hizmet Alım Güvenliği	1. Mal ve hizmet alımlarında ilgili mevzuatlara aykırı olmayacak bir şekilde uyulması gereken bilgi güvenliği kurallarının tanımlanması, bahse konu kuralların kurum tarafından hazırlanan tedarik dokümanlarına (teknik ve idari şartnamelere) eklenmesi 2. Farklı kuruluşlar ve üçüncü taraflarla yapılacak kurumsal gizlilik sözleşmelerinin hazırlanması	1. Kurum bünyesinde hazırlanan teknik ve/veya idari şartnamelere bilgi güvenliği ile ilgili hususların konulduğuna dair kayıtlar (tamamlanmış satın alma faaliyetinde kullanılmış iki adet teknik/idari şartname) 2. Yükleniciler ile yapılmış, imzalı iki adet Kurumsal Gizlilik Sözleşmesi
9	Zararlı Yazılımlardan Korunma	1. Kuruma ait sunucu ve istemci bilgisayarların lisans gerektirmeyen veya lisanslı bir virüs koruma yazılımı ile korunması 2. Bilgisayarlara yüklenen virüs koruma ajanlarının ve virüs tanıma dosyalarının güncel halde tutulması	Kuruma ait iki adet sunucu ve 5 adet istemci bilgisayardan alınan total virüs tarama iz kayıtları

S.No	Değerlendirme Yapılacak Başlık	Değerlendirilecek Başlık Kapsamında Kurumlar Tarafından Yapılması Beklenen Faaliyetler	Değerlendirilecek Başlık Kapsamında Hastane/İSM tarafından İSM/SBSGM'ye Gönderilecek Dokümanlar
10	Kullanıcıların Bilgi Güvenliği Sorumlulukları/ Elektronik Posta Güvenliği	1. Kurumsal / tüzel e-posta hesapları (e-posta alma, gönderme vb) ve internet kullanımıyla ilgili uyulması gereken bilgi güvenliği kuralları belirlenmesi ve bir prosedür olarak yayımlanması 2. Kurumun çeşitli alt birimleri için açılmış olan tüzel e-posta hesaplarının yönetiminin yapılması (bu maksatla oluşturulmuş posta kutularının paylaşılan (ortak) e-posta haline getirilmesi, aktif olarak kullanılmayan tüzel hesapların kapatılması)	1. İnternet ve e-posta kullanım prosedürü 2. Kurum bünyesinde kullanılan Tüzel e-posta hesaplarının listesi ve kullanım durumları
11	Sosyal Mühendislik ve Sosyal Medya Güvenliği	1. Sosyal mühendislik zafiyetleri engellemek ve sosyal medya güvenliğini sağlayabilmek için gerekli eğitimlerin verilmesi 2. Sosyal medya güvenliği ve sosyal mühendislik zafiyetlerine karşı alınacak önlemlerin politika metni olarak yayımlanması	Konu ile ilgili hazırlanan onaylı doküman.
12	Parola Güvenliği	Kurum personelinin uyması gereken parola politikalarının yer aldığı bir dokümanın hazırlanması	1. Kurum Parola Politikası 2. Politika çerçevesinde yapılan iş ve işlemler ile ilgili tutanaklar (Örneğin kurum etki alanı grup politikası parola politikası ekran görüntüleri, SBYS yazılımlarında parola yönetim politikasının uygulandığı ilgili ekranların çıktısı
13	Sunucu / Sistem Odası Güvenliği	Kuruma ait sunucular, iletişim cihazları (ana omurga anahtar, ana dağıtım panelleri vb.) ve SBA kapsamında kullanılan cihazların (yönlendirici, güvenlik duvarı)	Kurumun sistem odasının fiziki şartlarını gösteren her türlü kanıt (fotoğraf, kamera kaydı iz bilgileri, bakım kayıtları vb.)

S.No	Değerlendirme Yapılacak Başlık	Değerlendirilecek Başlık Kapsamında Kurumlar Tarafından Yapılması Beklenen Faaliyetler	Değerlendirilecek Başlık Kapsamında Hastane/İSM tarafından İSM/SBSGM'ye Gönderilecek Dokümanlar
		konumlandırıldığı sunucu ve sistemci odalarının fiziksel şartlarının iyileştirilmesi	
14	Yedekleme Yönetimi	1. Kurumsal veri ve bilgilerin saklanması ile ilgili genel hususların açıklandığı bir yedekleme politikası oluşturulması 2. Kurum yedekleme politikası uyarınca yedekleme planı hazırlanması 3. Yedekleme planı uyarınca alınan yedeklerin kontrolü için yedekleme kontrol listesi hazırlanması 4. Alınan yedeklerin yılda en az iki kez olacak şekilde geri dönüş testi yapılması	1- Kurum yedekleme politikası 2- Kurum yedekleme planı 3- Yedekleme kontrol listesi (doldurulmuş) 4- Yapılan geri dönüş testlerine ait bir adet tutanak
15	Web Sitelerinde SSL Sertifikası Kullanılması	1. Sağlık Bilgi Sistemleri Genel Müdürlüğü dışında bir başka yer sağlayıcıdan web sitesi hizmeti alınıyorsa veya bu hizmet doğrudan ilgili kurum tarafından sağlanıyorsa, söz konusu site/adresin güvenli iletişim ve sunucu doğrulama için SSL sertifikası olması Not: Hastanelerin laboratuvar sonuçlarının bildirimlerinin yapıldığı sayfalar da bu kapsamda değerlendirilecektir.	1. Adres çubuğu görünecek şekilde ilgili site/sayfanın herhangi bir tarayıcı yazılımından alınan ekran görüntüsü 2. İlgili sitede kullanılan sertifikaya ait ekran görüntüsü

TEŞEKKÜRLER

İZMİR İL SAĞLIK MÜDÜRLÜĞÜ

BİLGİ İŞLEM BİRİMİ

izmir.bilgiislem@saglik.gov.tr

EYLÜL 2018