BİLGİ GÜVENLİĞİ İLE İLGİLİ KRİTERLERİN DEĞERLENDİRME ESASLARI

1. Yılda En Az Bir Kez Bilgi Güvenliği Eğitimi Alan Personel Oranı

Personele bilgi güvenliği farkındalık eğitimi verilmesi ile ilgili hususlar;

- "Destek Hizmetleri" sözleşmeli pozisyonunda çalışan personelin değerlendirilmesinde kullanılan "TT.DH.3 İl Genelindeki Tüm Kurumların Bilgi Güvenliği Politikalarına Uyum Oranı" göstergesi kapsamında İSM'ler için belirlenen 2 nolu başlıkta (İl Sağlık Müdürlüğüne doğrudan bağlı birimlerde çalışan personele bilgi güvenliği farkındalık eğitimi verilmesi),

- "İdari Mali Hizmetler ADSM ve ADSH" sözleşmeli pozisyonunda çalışan personelin değerlendirilmesinde kullanılan "TT.İMHM.10 Hastane Bilgi Güvenliği Konusunda Tüm Personele Yılda En Az Bir Kez Eğitim Verilmesi" göstergesinde,

- "İdari Mali Hizmetler" sözleşmeli pozisyonunda çalışan personelin değerlendirilmesinde kullanılan "TT.İMHM.ADSM.ADSH.10 Hastane Bilgi Güvenliği Konusunda Tüm Personele Yılda En Az Bir Kez Eğitim Verilmesi" göstergesinde,

- "İlçe Sağlık Müdürlüğü" sözleşmeli pozisyonunda çalışan personelin değerlendirilmesinde kullanılan "TT.İLÇESM.8 İlçe Genelinde Birinci Basamak Sağlık Kuruluşlarında Bilgi Güvenliği Konusunda Eğitim Verilen Personel Oranı" göstergesinde tanımlanmıştır.

Bu dokümanda yer almayan konular için (eğitimler kime verilecek, puanlama nasıl yapılacak vb.) SYPD Yönergesinin ekinde yer alan ilgili göstergelerde yazan hususlara dikkat edilmesi gerekmektedir.

Bilgi güvenliğinin bilgi sistem güvenliğinden daha geniş bir kavram olması; personel güvenliği, evrak güvenliği, fiziki güvenlik gibi konuları da içermesi nedeniyle eğitimin sadece bilgisayar kullanan kişilere değil, kurum tarafından işlenen bilgiler ile bu bilgilerin işlendiği sistem ve tesislere erişen tüm personele verilmesi gerekmektedir.

Sağlık tesislerinde işlenen verilerin ağırlıklı olarak kişisel veriler ve kişisel verilerin daha da özel koruma gerektiren bir parçasını oluşturan sağlık verisi olması nedeniyle, bu verilere erişim ihtimali olan tüm personelin eğitim planlamasına alınması uygun olacaktır. Eğitim içeriği hazırlanırken **bilgi sistem güvenliği ile ilgili konulara ilave olarak başta kişisel veriler ve sağlık verilerinin korunması olmak üzere diğer konuların da mutlaka dikkate alınması** önem arz etmektedir.

Eğitimin içeriği hazırlanırken Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesinde yer alan ana esaslar ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunda yer alan ve son kullanıcıları doğrudan ilgilendiren başlıkların (**kurum bilgi güvenliği organizasyonu, insan kaynakları güvenliği kapsamında işe başlama, görev değişikliği ve işten ayrılma süreçlerinde dikkat edilmesi gereken hususlar, bilgi güvenliği farkındalık bildirgesi içeriği, e-posta güvenliği, parola kullanımı, sosyal medya kullanımı, sosyal mühendislik saldırıları ve oltalama e-postalarından korunma, kişisel verileri koruma kanunu kapsamında çalışanların sorumlulukları, ihtiyaç olduğunda bilgisayarlardaki verilerin güvenli olarak silinmesi ve güvenli imha işlemleri, taşınabilir medya kullanımı, kurum bilgisayarlarının iş dışında kullanımı prensipleri, kurum dışı ağlar/kablosuz ağlar kullanılırken dikkat edilecek hususlar, bilgi güvenliği ihlal bildirimlerinin ne şekilde yapılacağı, fiziki güvenlik kapsamında dikkat edilecek hususlar, kurum bilgi kaynaklarına uzaktan erişim, lisanslı yazılım kullanımı vb.**) dikkate alınması gerekmektedir.

Farkındalık eğitimleri yüz yüze, kurumların kendi uzaktan eğitim sistemleri üzerinden veya Bakanlığımız Uzaktan Sağlık Eğitim Sistemi (USES) üzerinden yapılabilecektir. Eğitimlerin ideal şartlarda yüz yüze eğitim şeklinde yapılması tercih edilmekle beraber uzaktan eğitim şeklinde verilmesinde de bir mahzur bulunmamaktadır.

SYPD Yönergesinde bu gösterge için veri toplama ve analiz periyodu bir yıl olarak belirlenmiştir. Bu kapsamda tüm kurumlarımız tarafından bünyelerinde çalışan tüm personel dikkate alınarak bilgi

güvenliği farkındalık eğitimleri planlanacak, icra edilecek ve eğitim yapıldığına dair kayıtlar tutulacaktır.

Eğitimlerin yapıldığına dair kayıtların geçmiş yıllardan farklı olarak ÇKYS/İKYS'ye değil 2024 yılı başında hizmete verilen Entegre Kurumsal İletişim Platformuna (EKİP) girilmesi gerekmektedir.

Bu gösterge için hesaplama yapılırken;

o İlgili kartların Yönetim Hizmetleri Genel Müdürlüğü / Yönetim Hizmetleri Dairesi Başkanlığının web sayfasında (https://yhgm.saglik.gov.tr/TR-34890/yonetim-izleme-ve-degerlendirme-dairesi-baskanligi.html) yayımlanan en son sürümlerinde yazan kriterler dikkate alınacaktır.

o Hesaplama yapılırken 31 Aralık 2024 tarihi itibarı ile ilgili kurumun "aktif" personel mevcudu ve bu personelin 01 Ocak 2024-31 Aralık 2024 tarihleri arasında eğitim alıp almadığına bakılacaktır. Eğitimin hangi kurum tarafından verildiği önemli değildir. Personelin herhangi bir kurumdan bir kez eğitim alması yeterli olacaktır.

o Hesaplamaların doğru sonuçlar vermesi için ilgili kurumların personel ayrılış ve katılış işlemlerinin doğru ve zamanında EKİP sistemine girilmiş olması büyük önem arz etmektedir. İtiraz safhasında, hesaplamanın kurumların personel kayıtlarındaki eksik ve hatalardan kaynaklandığının tespit edilmesi halinde, yapılacak müracaatlar kabul edilmeyecektir.

o **Eğitimlerin Bakanlığımız USES veya kurumların kendi bünyelerinde mevcut uzaktan eğitim sistemleri üzerinden verilmesi halinde, EKİP ile bahse konu sistemler arasında doğrudan bir entegrasyon olmadığı dikkate alınarak, eğitim girişlerinin yukarıda belirtildiği şekilde ayrıca EKİP'e de girilmesi gerektiği dikkate alınacaktır.**

2. İl Genelindeki Tüm Kurumların Bilgi Güvenliği Politikalarına Uyum Oranı

Göstergede yer alan "**İl Genelindeki Kurumlar**" ifadesi 2024 yılı için "**E kategorisindeki hastaneler, ADSM/ADSH'ler dâhil tüm 2 ve 3'ncü basamak kamu hastaneleri**" olarak uygulanacaktır. **1'nci basamak sağlık tesisleri bu başlık kapsamında yer almamaktadır**.

Bilgi güvenliği politikaları ile uyum kapsamında İl Sağlık Müdürlüğünün kendisi ve ilgili kamu hastanelerince, Ek-1'de yer alan başlıklarda açıklanan konuları gerçekleştirmeleri ve bunun delili olarak yine Ek-1'de belirtilen çıktıların üretilmesi ve sunulması beklenmektedir.

Kurumların SYPD işlemleri açısından bu göstergeden "başarılı/uyumlu" sayılabilmeleri için başlıklar için belirlenen puanlar dikkate alınarak toplamda (100 tam puan üzerinden) en az 80 puana ulaşmaları, ayrıca zorunlu başlık olarak belirlenen "Bilgisayarların merkezi olarak yönetim ve denetimi işlemleri" başlığını tamamlamış olmaları gerekmektedir.

Her bir başlık için değerlendirme yapılırken, ilgili başlık için belirlenen işlemlerin tümünün yapılması gerekmekte olup bir başlık için istenen bilgi ve belgelerden birinin bile eksik olması halinde, ilgili kuruma söz konusu başlıktan "0 (sıfır)" puan verilecektir. Bir başka ifade ile başlıklara "0" ya da "tam" puan verilecektir.

Kapsam dâhilinde yer alan tüm kurumlarca, Ek-1'de belirtilen başlıklar ile ilgili çalışma yapılacak, yapılan çalışmaların sonuçları (İSM'ler tarafından belirlenecek bir tarihe kadar) İSM'ye gönderilecektir.

Bu gösterge için illerin genel başarı durumları hesaplanırken, illerin kategorileri (İ1-İ7) ve hastane sayıları dikkate alınarak SBSGM tarafından belirlenecek sayıda kurumun belgeleri üzerinden değerlendirme yapılacak, hesaplanan oran il geneline yansıtılacaktır.

Örneklemde yer alacak kurumlar (İSM'lerin kendisi mutlaka örneklem içinde yer alacak şekilde) SBSGM tarafından seçilecek ve **24 Aralık 2024 Salı günü** Genel Müdürlüğümüz bilgi güvenliği web sayfasında (https://bilgiguvenligi.saglik.gov.tr/Home/BGPerformansDegerlendirmesi adresinde) yayımlanacak ayrıca Bakanlığımız e-posta sistemi üzerinden İSM'lerde görev yapan bilgi sistemleri koordinatörleri ve bilgi güvenliği yetkilisi/yedeklerine gönderilecektir.

İSM'lerin kendisine ve örnekleme dâhil edilen hastanelerine ait bilgi ve belgeler en geç **27 Aralık 2024 Cuma günü mesai bitimine kadar** tarihine kadar elektronik ortamda SBSGM'ye gönderilmiş olacaktır.

İSM'nin kendisi ve örneklemde yer alan kurumların evrakları, Genel Müdürlüğümüzün ilgili birimleri (BGYS, SOME, Bilişim Teknik Destek ve E-Posta Yönetimi) tarafından incelenecek ve yukarıda belirtilen esaslar doğrultusunda puanlama yapılacaktır. Bu safhada gerekiyorsa ilgili kurumlarda çalışan personel ile birebir temas kurularak ilave bilgi ve belge istenebilecektir.

Hastaneler tarafından İSM'lere gönderilen kayıtlar, ihtiyaç olması durumunda örnekleme usulü ile yapılacak denetimlerde kullanılmak üzere, bir sonraki yılın Temmuz ayına kadar İSM tarafından saklanacaktır.

3. Ek-1 Başlıkların "İl Sağlık Müdürlükleri ve Birimleri Kurum Hizmet ve Teşvik Ek Ödeme Yönergesi" Uyarınca Yapılacak Ek Ödemeler İçin Kullanılma Esasları

Ek-1'de sıralanan başlıklardan İSM'ler ile ilgili olanlar, Sağlık Bakanlığı "İl Sağlık Müdürlükleri ve Birimleri Kurum Hizmet ve Teşvik Ek Ödeme Yönergesi" uyarınca İSM'lerde çalışan personele yapılacak ek ödemelere esas olmak üzere İSM Birim Performans Kriteri olarak kullanılacaktır.

Ek-1'deki başlıkların İSM kurum hizmet hedefleri açısından puanları aşağıdaki tabloda olduğu gibidir. İSM'ler için hesaplanan puanlar 2025 yılı şubat ayı içerisinde Yönetim Hizmetleri Genel Müdürlüğüne (Mali Hizmetler Daire Başkanlığı) ve İl Sağlık Müdürlüklerine resmi yazı gönderilecektir. Gönderilen puanlar İSM'de çalışan personelin 2025 yılı ek ödeme hesaplamasına esas olacaktır. Puanlama yapılırken aşağıdaki tabloda belirtilen değerler esas alınacaktır.

Bilgi güvenliği başlıkları için belirlenen 50 puan, İSM Birim Performans Kriterlerinin tamamı için belirlenen toplam performans puanının (2000 puan) % 2,5'ini oluşturmaktadır.

S.No.	Değerlendirme Yapılacak Başlık	Puan
1	Tedarikçi ilişkilerinde bilgi güvenliği işlemleri	**5**
2	İl Sağlık Müdürlüğüne doğrudan bağlı birimlerde çalışan personele bilgi güvenliği farkındalık eğitimi verilmesi	**5**
3	İl genelinde görev yapan tüm personelin oltalama tatbikatlarındaki davranışı	**2.5**
4	Sektörel SOME tarafından e-posta, resmi yazı vb. yöntemlerle İSM Kurumsal SOME'lere bildirilen ihlal olaylarına süresi içerisinde işlem yapılması	**5**
5	USOM tarafından SOME İletişim Platformuna (SİP) girilen ihlal bildirimlerine süresi içerisinde işlem yapılması	**5**
6	Kurumsal E-Posta kullanıcı sayısının artırılması	**2,5**
7	Kurumsal E-Posta kullanım etkinliğinin artırılması	**2,5**
8	Bilgisayarların merkezi olarak yönetim ve denetimi işlemleri	**10**
9	İşletim sistemi güncelleme işlemleri	**5**
10	Zararlı yazılımlardan korunma işlemleri	**7.5**
Toplam		**50**