SYPD TT.DH.3. GÖSTERGESİ 2022 YILI BAŞLIKLARI

S.No	Değerlendirme Yapılacak Başlık	Yapılması Beklenen Faaliyetler	Gönderilecek Bilgi ve Belgeler	Puanı	
				İSM	HST
1	Tedarikçi ilişkilerinde bilgi güvenliği işlemleri	**Bu başlık kapsamında hem İSM'ler, hem de Hastane/ADSM'ler değerlendirilecektir.** Bu başlık kapsamında; 1. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) Başkanlığı Bilgi ve İletişim Güvenliği Rehberi'nin "**Tedarikçi İlişkileri Güvenliği**" başlıklı 3.5.3 maddesi ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu'nun "**Mal ve Hizmet Alımları Güvenliği**" başlıklı 11.1. maddesi uyarınca; - Yükleniciye, özel koruma ihtiyacı olan veri/bilgilerin teslim edilmesi, - Özel koruma ihtiyacı olan veri/bilgilerin işlendiği ortamlarda fiziki olarak yüklenici personeli çalıştırılması, - Kurumun bilişim sistemlerine (uzaktan erişimler dâhil) yüklenici personeli tarafından erişim yapılması ihtiyacı olması, halinde ihale dokümanlarına bilgi güvenliği ile ilgili gereksinimlerin ilave edilmesi, 2. Ayrıca satın alınacak yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğine dair taahhütname (**açık kapı taahhütnamesi**) alınması gerekmektedir. ***Detaylar için dipnot***[1]	Bu başlık için Genel Müdürlüğümüze herhangi bir bilgi ve belge gönderilmeyecektir. İhale dokümanlarında bahse konu girdilerin yapılıp yapılmadığı, tarafımızdan Elektronik Kamu Alımları Platformunda (EKAP) yer alan ihale dokümanlarının incelenmesi suretiyle kontrol edilecektir. EKAP'tan inceleme yapılırken, ihtiyaç sahibi birim değil ihaleyi yapan birim dikkate alınacaktır. Örneğin bir devlet hastanesi ihtiyacı için alım yapılmış ancak ihale İSM tarafından gerçekleştirilmiş ise, değerlendirme sonucu İSM için geçerli olacaktır.	**15**	**10**

[1] Bilgi güvenliği gereksinimleri ile ilgili hususların sadece bilişim/bilgi sistemleri ile ilgili mal ve hizmetlerin tedarik işlemlerinde değil, **başta kişisel sağlık verileri olmak üzere hassas verilerin işlenmesi söz konusu olan tüm mal ve hizmet alımları** (Sonuç Karşılığı Laboratuvar Hizmet Alımı, Nükleer Tıp Görüntüleme Hizmeti Alımı, Bilgisayarlı Tomografi Tetkik Başı Hizmet Alımı, Puan Karşılığı Görüntüleme Tıbbi Cihazı ve Tıbbi Hizmetleri Alımı, PACS ve RIS Teleradyoloji Hizmet Alımı, MRI ve BT Teleradyoloji Yöntemiyle Radyolojik Tetkikler Raporlandırma Hizmeti Alımı vb.) için hazırlanan ihale dokümanlarında (sözleşme, idari şartname veya teknik şartname) yer

S.No	Değerlendirme Yapılacak Başlık	Yapılması Beklenen Faaliyetler	Gönderilecek Bilgi ve Belgeler	Puanı	
				İSM	HST
2	İl Sağlık Müdürlüğüne doğrudan bağlı birimlerde çalışan personele bilgi güvenliği farkındalık eğitimi verilmesi	**Bu başlık kapsamında sadece İSM'ler değerlendirilecektir.** SYPD kapsamında Hastane, ADSM ve 1'nci basamak sağlık tesislerinde çalışan personele yıllık olarak verilmesi gereken bilgi güvenliği farkındalık eğitimleri, TT.İLÇESM.8 (İlçe Genelinde Birinci Basamak Sağlık Kuruluşlarında Çalışan Personele Yılda En Az Bir Kez Eğitim Verilmesi), TT.İMHM.10 (Hastane Bilgi Güvenliği Konusunda Tüm Personele Yılda En Az Bir Kez Eğitim Verilmesi) ve TT.İMHM.ADSM.ADSH.10 (Hastane Bilgi Güvenliği Konusunda Tüm Personele Yılda En Az Bir Kez Eğitim Verilmesi) göstergeleri ile değerlendirilmektedir. Bu başlık kapsamında, bahse konu üç göstergenin kapsamında yer almayan diğer personele (İSM'ye bağlı başkanlıklar, il halk sağlığı laboratuvarı ve il ambulans servisi başhekimliğine bağlı birimler – tüm 112 acil sağlık istasyonları dâhil) verilen bilgi güvenliği farkındalık eğitimlerinin ölçülmesi hedeflenmiştir. Bu başlık uyarınca kapsam dâhilinde yer alan personele verilen eğitimlerin oranının % 75 veya üzeri olması halinde, İSM bu başlıktan başarılı olmuş sayılacaktır.	Bu başlık için Genel Müdürlüğümüze herhangi bir bilgi ve belge gönderilmeyecektir. Yapılan Eğitimlerin kayıtları ÇKYS/İKYS→Eğitim Ana Menüsü→Personel Hizmet İçi Eğitim Bilgileri→Sağlık Tesisleri Eğitimleri (71)→Bilgi Güvenliği (9)→Çalışan ve Hasta Bilgi Güvenliği menüsü kullanılarak sisteme girilecektir. Yıl içerisinde atama gören personel, eski kurumunda bilgi güvenliği eğitimi almış ve alınan bu eğitim ÇKYS/İKYS/Eğitim modülüne işlenmiş ise, personele yeni kurumunda ayrıca eğitim verilmesine gerek bulunmamaktadır. Hesaplama 31 Aralık 2022 tarihi itibarı ile kapsam dâhilinde yer alan kurumlarda görev yapan aktif personel mevcudu dikkate alınarak yapılacaktır. **Eğitimlerin ÇKYS/İKYS'ye girilmesi zorunludur. Süresi içerisinde ÇKYS/İKYS'ye girilmemiş veriler dikkate alınmayacaktır.**	**15**	**0**
3	İhlal bildirimlerine süresi içerisinde işlem yapılması	**Bu başlık kapsamında sadece İSM'ler değerlendirilecektir.** Bu başlık kapsamında değerlendirme yapılırken; 1. Bakanlığımız Sektörel SOME'si, Ulusal Siber Olaylara Müdahale (USOM) siber İletişim Platformu (SİP) ve CBDDO Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi tarafından İSM'lerde faaliyet gösteren Kurumsal SOME'lere bildirilen siber olay bildirimlerinin süresi içerisinde kapatılması,	Bu başlık için Genel Müdürlüğümüze herhangi bir bilgi ve belge gönderilmeyecek, değerlendirme işlemi Genel Müdürlüğümüz SOME Birimi tarafından yapılacaktır. Bu başlıkla ilgili konular için some@saglik.gov.tr ile iletişim kurulacaktır.	**10**	**0**

alması beklenmektedir. Yüklenicinin hiçbir şekilde hassas bilgi ve verilere erişimi olmayan mal ve hizmet alımlarında, şartnamelerde bilgi güvenliği ile ilgili hususların yer almasına gerek bulunmamaktadır.

S.No	Değerlendirme Yapılacak Başlık	Yapılması Beklenen Faaliyetler	Gönderilecek Bilgi ve Belgeler	Puanı	
				İSM	HST
		2. Elde olmayan nedenlerle süresi içerisinde işlem yapılamayan siber olaylara neden işlem yapılmadığının Bakanlık Sektörel SOME'ye (SOME Birimine / some@saglik.gov.tr) bildirilmesi konuları dikkate alınacaktır.			
4	Bilgi güvenliği risk yönetimi işlemleri	**Bu başlık kapsamında hem İSM'ler, hem de Hastane/ADSM'ler değerlendirilecektir.** İSM ve Hastane/ADSM'ler tarafından kendi kurumları ile ilgili bilgi varlıkları/bilgi işleme süreçleri dikkate alınarak bilgi güvenliği risk çalışması yapılacak, tespit edilen riskler "Risk Tablosu/Risk İyileştirme Planı"na işlenecek ve risklerin takip edilmesi sağlanacaktır. Risk Tablosunda/Risk İyileştirme Planında bilgi güvenliğine (bilginin gizlilik, bütünlük ve erişilebilirliğini tehdit oluşturan) riskler yazılacaktır. Risk analiz çalışmalarında **en az fiziksel güvenlik, sistem odası güvenliği, sunucu güvenliği, insan kaynakları güvenliği, veri tabanı güvenliği, HBYS uygulaması güvenliği** gibi konuları içerecek şekilde kurum/hastane risklerinin belirlenmesi gerekmektedir.	**Bilgi Güvenliği Risk Tablosu/Risk İyileştirme Planı** İSM ve Hastane/ADSM'ler tarafından ayrı ayrı gönderilecektir. Örnek olarak Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu ekinde yer alan risk iyileştirme planı esas alınabilecek veya hastanelerde sağlıkta kalite sistemi (SKS) denetimleri kapsamında gerçekleştirilen risk çalışmalarında hazırlanan risk tablosu kullanılabilecektir. **Farklı kurumlar tarafından aynı tablo/planın gönderilmesi halinde, aynı dokümanı kullandığı tespit edilen tüm kurumlar bu başlıktan başarısız sayılacaktır.** Kurumda etkin bir şekilde bilgi güvenliği risk yönetimi yapılmadığı (yan sütunda belirtilen alanlara ilişkin riskleri içermeyen, sadece hasta ve çalışan güvenliğine ilişkin risklerin tanımlandığı, genel-geçer ifadelerle kaleme alınmış kısıtlı sayıda risk bulunan) kanaati uyandıran çalışmalar başarısız olarak kabul edilecektir.	**10**	**10**
5	Bilgisayarların merkezi olarak yönetim ve denetimi işlemleri	**Bu başlık kapsamında hem İSM'ler, hem de Hastane/ADSM'ler değerlendirilecektir.** Kurumun kullanıcı ve bilgisayarlarının merkezi olarak yönetim ve denetimlerinin yapılmasını sağlayacak (etki alanı veya benzeri) bir bilgi sistem altyapısı kurulması, tüm kullanıcı ve bilgisayarların bu	**1. İSM'nin geneli için (hastanelerde kurulu olanlar da dâhil) bu başlık kapsamında alınan tedbirleri açıklayan aşağıdaki soruların yanıtlarını açıklayan özet bir rapor**	**20**	**20**

S.No	Değerlendirme Yapılacak Başlık	Yapılması Beklenen Faaliyetler	Gönderilecek Bilgi ve Belgeler	Puanı	
				İSM	HST
		yapıya dâhil edilerek belirlenecek kurumsal bilgi güvenliği politikalarına uymaya zorlanması	- Tek bir etki alanı[2] mı mevcuttur? - Değil ise hangi kurumlarda fiilen etki alanı sunucusu çalıştırılmaktadır? - Kurulan etki alanının (alanlarının) adı (adları) nedir? - Kaç adet DC sunucusu mevcuttur? - Ne kadarı fiziksel ne kadarı sanal sunucu şeklindedir? - Sunucuların IP adresleri ve makine adları nedir? - Hangi sunucular hangi kurumlara hizmet etmektedir? sorularının cevabını içerecek şekilde) Bu rapor (ilin tamamı için) İSM tarafından gönderilecektir. **2. Seçilen kurumdaki kullanıcılar ve bilgisayarların etki alanında olduğunu gösteren OU görüntüleri** İSM ve hastane/ADSM'ler tarafından ayrı ayrı gönderilecektir. **3. Genel etki alanı politikası (global domain policy) dosyası** Etki alanı işleten kurumlar tarafından (html veya pdf formatında) gönderilecektir.		
6	İşletim sistemi güncelleme işlemleri	**Bu başlık kapsamında hem İSM'ler, hem de Hastane/ADSM'ler değerlendirilecektir.** Bu başlık kapsamında ilgili kurumlarda sunucu ve istemci bilgisayarlarda kullanılan işletim sistemi yazılımlarının, kurumların bünyesinde merkezi veya dağıtık olarak kurulmuş yerel	**1. İl geneli için tüm sağlık tesislerini içerecek şekilde bu başlık kapsamında alınan tedbirleri açıklayan bilgi notu** İSM tarafından gönderilecektir. **2. Seçilen kurumda kullanılan bilgisayarların otomatik güncelleme kapsamına alındığını gösterir yerel dağıtım noktaları/sunucuları yönetim arayüzlerinde alınan ekran görüntüleri**	**10**	**10**

[2] Bu başlıkta geçen etki alanı/DC vb. terim ve kısaltmalar, kurumları belli bir teknolojiye zorlamak amacıyla kullanılmamıştır. Kurumlar bahse konu sistem ve altyapıyı herhangi bir yazılım/araç/sistem kullanarak yapabilecektir.

S.No	Değerlendirme Yapılacak Başlık	Yapılması Beklenen Faaliyetler	Gönderilecek Bilgi ve Belgeler	Puanı	
				İSM	HST
		dağıtım noktaları/sunucuları (SSCM, WSUS vb.)[3] üzerinden otomatik olarak güncellenmesi için tedbir alınması gerekmektedir. **Kurum envanterinde yer alan bilgisayar sayısı 100'den az olan kurumlarda,** bilgisayarları doğrudan internette bulunan güncelleme sunucularına bağlamak suretiyle veya bilgisayarları tek tek manuel olarak güncelleme yapabilecektir.	İSM ve hastane/ADSM'ler tarafından ayrı ayrı gönderilecektir. **3. Bilgisayarları doğrudan internete bağlamak suretiyle veya manuel olarak tek tek güncelleme yapan kurumlar için güncelleme işlemlerinin ne şekilde gerçekleştirildiği ve konuyla ilgili sorumlulukların tanımlandığı onaylı bir talimat ve dipnotta[4] açıklandığı şekilde hazırlanan bir tutanak.** Bu şekilde güncelleme yapan kurumlar tarafından gönderilecektir.		
7	Zararlı yazılımlardan korunma işlemleri	**Bu başlık kapsamında hem İSM'ler, hem de Hastane/ADSM'ler değerlendirilecektir.** Bu başlık kapsamında ilgili kurumlarda istemci bilgisayarlarda kullanılan zararlı yazılımlarla mücadele (virüs koruma) yazılımlarının ve virüs tanımla dosyalarının, kurumların bünyesinde merkezi veya dağıtık olarak kurulmuş yerel dağıtım noktaları/sunucuları üzerinden otomatik olarak güncellenmesi için tedbir alınması gerekmektedir. **Kurum envanterinde yer alan bilgisayar sayısı 100'den az olan kurumlarda,** bilgisayarları doğrudan internette bulunan güncelleme sunucularına bağlamak suretiyle veya bilgisayarları tek tek manuel olarak güncelleme yapabilecektir.	**1. İl geneli için tüm sağlık tesislerini içerecek şekilde bu başlık kapsamında alınan tedbirleri açıklayan bilgi notu** İSM tarafından gönderilecektir. **2. Seçilen kurumda kullanılan bilgisayarların otomatik güncelleme kapsamına alındığını gösterir yerel dağıtım noktaları/sunucuları yönetim arayüzlerinde alınan ekran görüntüleri** İSM ve hastane/ADSM'ler tarafından ayrı ayrı gönderilecektir. **3. Bilgisayarları doğrudan internete bağlamak suretiyle veya manuel olarak tek tek güncelleme yapan kurumlar için güncelleme işlemlerinin ne şekilde gerçekleştirildiği ve konuyla ilgili**	**10**	**10**

[3] Bu başlıkta geçen SSCM/WSUS gibi kısaltmalar, kurumları belli bir teknolojiye zorlamak amacıyla kullanılmamıştır. Kurumlar bahse konu sistem ve altyapıyı herhangi bir yazılım/araç/sistem kullanarak yapabilecektir.

[4] Bu durumda olan kurumlarca, kurum envanterinde yer alan bilgisayar sayısının 100'den az olduğuna dair taşınır kayıt birimi yetkilisi ve İSM'ler için destek hizmetleri başkanı, Hastane/ADSM'ler için idari ve mali işler müdürünün imzasının yer alacağı bir tutanak hazırlanacak ve hazırlanan tutanak bu başlık için istenen belgelerle birlikte Genel Müdürlüğümüze gönderilecektir. MKYS üzerinden yapılacak kontrollerde, kurum envanterinde 100'den fazla bilgisayar bulunduğunun tespit edilmesi halinde, ilgili kurum bu başlıktan başarısız olarak kabul edilecektir.

S.No	Değerlendirme Yapılacak Başlık	Yapılması Beklenen Faaliyetler	Gönderilecek Bilgi ve Belgeler	Puanı	
				İSM	HST
			sorumlulukların tanımlandığı onaylı bir talimat ve dipnotta açıklandığı şekilde hazırlanan bir tutanak Bu şekilde güncelleme yapan kurumlar tarafından gönderilecektir.		
8	IP dağıtımı işlemleri	**Bu başlık kapsamında hem İSM'ler, hem de Hastane/ADSM'ler değerlendirilecektir.** Bu başlık kapsamında sabit IP verilmesi gerekmeyen tüm cihazların IP dağıtım işlemlerinin DHCP servisi vasıtası ile otomatik olarak yapılması beklenmektedir. **Kurum envanterinde yer alan bilgisayar sayısı 100'den az olan kurumlarda** bilgisayarlara manuel IP dağıtımı yapılabilecektir.	**1. İl genelinde IP dağıtım işlemlerinin hangi cihazlar/sistemler vasıtasıyla nasıl (merkezi, dağıtık vb.) yapıldığını açıklayan bilgi notu** İSM tarafından gönderilecektir. **2. DHCP servisinin çalıştığı sunucudaki DHCP uygulaması yönetim ekranlarına ait ekran görüntüleri** Seçilen tüm kurumlar tarafından IP Scope bilgilerini içerecek şekilde ayrı ayrı gönderilecektir. **3. Manuel IP dağıtımı yapan kurumlar için IP dağıtım ve güncelleme işlemlerinin ne şekilde yapıldığını açıklayan onaylı bir talimat ve dipnotta açıklandığı şekilde hazırlanan bir tutanak** Bu şekilde IP dağıtımı yapan kurumlar tarafından gönderilecektir.	**10**	**10**
9	SBYS/HBYS erişim yetki ve kontrol matrisi hazırlanması ve güncel halde bulundurulması	**Bu başlık kapsamında sadece Hastane/ADSM'ler değerlendirilecektir.** Bu başlık kapsamında hastanelerden, Kişisel Verileri Koruma Kurumu tarafından yayımlanan Kişisel Veri Güvenliği (Teknik ve İdari Tedbirler) Rehberinin 3.1 maddesi ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunun A.6 Erişim Kontrolü maddesinde açıklandığı şekilde, SBYS/HBYS kullanıcılarının bu sistemlerde saklanan kişisel verilere erişimi için verilen yetkileri	**Erişim yetki kontrol matrisi** Hastane ve ADSM'ler tarafından ayrı ayrı gönderilecektir.	**0**	**10**

S.No	Değerlendirme Yapılacak Başlık	Yapılması Beklenen Faaliyetler	Gönderilecek Bilgi ve Belgeler	Puanı	
				İSM	HST
		gösteren "**erişim yetki ve kontrol matrisi**[5]" hazırlamaları ve güncel halde bulundurmaları beklenmektedir.			
10	SBYS/HBYS iş sürekliliği işlemleri	**Bu başlık kapsamında sadece Hastane/ADSM'ler değerlendirilecektir.** Bu madde kapsamında, hastanelerde kullanılmakta olan SBYS/HBYS hizmetlerinin durmasına veya büyük oranda devre dışı kalmasına neden olabilecek (uygulama ve VTYS sunucularından, kurum sorumluluğunda bulunan ağ cihazlarından, şebeke elektriği/jeneratör/kesintisiz güç kaynağı/iklimlendirme gibi destekleyici altyapı hizmetlerinden kaynaklanan) bir olay/arıza meydana gelmesi halinde, sistemin yeniden normal fonksiyonları ile çalışır hale getirilmesi maksadıyla **Hastane/ADSM Bilgi İşlem Birimi** tarafından yapılacak işlerin açıklandığı iş sürekliliği planlarının hazırlanması beklenmektedir.	**1. SBYS/HBYS hizmeti için hazırlanmış iş sürekliği planı** Müstakil olarak SBYS/HBYS işleten kurumlar tarafından gönderilecektir. **2. 2022 yılında yapılmış SBYS/HBYS geri dönüş test kayıtları** SBYS/HBYS hizmetini merkezi olarak alan hastaneler tarafından bu başlık için herhangi bir bilgi/belge gönderilmeyecektir. Bu durumda, ilde merkezi SBYS/HBYS işleten kurumun aynı maksatla hazırlanmış olan bilgi ve belgelerinin İSM tarafından gönderilmesi beklenmektedir.	**0**	**10**
11	VLAN yapılanması	**Bu başlık kapsamında sadece Hastane/ADSM'ler değerlendirilecektir.** Bu başlık kapsamında Hastane/ADSM yerel alan ağında, ilgili kurum tarafından belirlenecek politikalar doğrultusunda alt sanal ağlar (VLAN) oluşturulması beklenmektedir. VLAN yapılanması için planlama yapılırken kurumda mevcut ağ cihazlarının miktarı ve özellikleri, kurumda kullanılan bilgisayar ve ağa bağlanan diğer cihazların miktarları, kurum binasının/binalarının fiziki yapısı (kat/blok sayısı ve yerleşimleri vb.), kurumda sunucu hizmeti verilip verilmediği gibi kriterler dikkate alınacaktır.	**1. Kurumun VLAN yapılanma esaslarını anlatan serbest metin tarzında bilgi notu.** **2. Kurum VLAN yapılanmasını gösteren mantıksal ağ topolojisi (IP detaylarını içermeyecek şekilde).** **3. Kurum ağında yer alan cihazların VLAN yapılanmasını desteklememesi halinde, bu ihtiyacın giderilmesi için kurum tarafından yapılan girişimlere ilişkin her türlü bilgi ve belge (teknik rapor, teknik şartname taslağı, ihtiyaç tespit komisyonu onayı, kaynak tahsisi için üst makamlara yapılan talep yazısı vb.)**	**0**	**10**

[5] Bu madde kapsamında kullanılabilecek örnek bir erişim yetki kontrol matrisi https://bilgiguvenligi.saglik.gov.tr/Home/BGPerformansDegerlendirmesi adresinde yayımlanacaktır. Hastane ve ADSM'ler bu dokümanı örnek almak suretiyle kendi erişim yetki kontrol matrislerini hazırlayacak ve hazırlanan dokümanın onaylı ve güncel olduğu ilgili makamlar tarafından onaylanacaktır.

S.No	Değerlendirme Yapılacak Başlık	Yapılması Beklenen Faaliyetler	Gönderilecek Bilgi ve Belgeler	Puanı	
				İSM	HST
		Bu başlık kapsamında asgari olarak kullanıcı bilgisayarları, sunucu bilgisayarları, (varsa) misafir ağı ve nesnelerin interneti cihazları (IP telefonlar/güvenlik kameraları/kartlı geçiş sistemleri vb.) için ayrı VLAN'ların tesis edilmesi gerekmektedir. Uç sayısına bağlı olarak özellikle kullanıcı bilgisayarlarının bağlantısında kullanılan ağın, daha fazla sayıda VLAN'lara ayrılması beklenmektedir.	Yukarıda belirtilen dokümanlar seçilen her bir kurum tarafından ayrı ayrı gönderilecektir.		
			Toplam	**100**	**100**