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)	<u>İSM'ler:</u> 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 <u>Hastaneler:</u> Bilgi güvenliği yetkilisi görevlendirmesi yapılmış ise konuyla ilgili görevlendirme yazısı <u>Açıklama:</u> 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	<u>İSM'ler:</u> 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 <u>Hastaneler:</u> Yukarıdakilere ilave olarak kurum parola politikasının SBYS'lerde de uygulandığına dair ilgili uygulamadan alınacak ekran görüntüleri veya benzeri deliller <u>Açıklama:</u> 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	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
		prosedür oluşturulması 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) konumlandırıldığı sunucu ve sistemci odalarının fiziksel	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
		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