Kodu	Yayın Tarihi	Revizyon No	Revizyon Tarihi	Sayfa Sayısı / Num.
BY.PR.14	20.11.2019	-	-	1/5

1. AMAÇ

Bu prosedürün amacı, T.C Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesislerin de satın alma süreçlerinin Sağlık Bakanlığı Bilgi Güvenliği Politikalarına uygun olarak yapılması için izlenecek yöntemi tanımlamaktır.

2. KAPSAM

Bu prosedür, T.C Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesislerinde bünyesinde görev yapan/yapacak tüm personeli (kamu personeli, tam zamanlı ya da yarı zamanlı olarak çalışan sözleşmeli personel, yüklenici firma çalışanları, iş ortaklarının çalışanları, destek alınan firmaların personeli vb.) ve T.C Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesisleri ile herhangi bir satın alma işlemi kapsamında yüklenici olarak işlem yapan tüm gerçek ve tüzel kişileri kapsar.

3. TANIMLAR

İSM: Ardahan İl Sağlık Müdürlüğü
Bağlı Sağlık Tesisleri: Kamu Hastaneleri, Toplum Sağlığı Merkezleri, Entegre Hastaneler, Halk Sağlığı Laboratuvarı, İl Ambulans Servis Başhekimliği
KTS: Kayıt Tescil Sistemi
HBYS:Hastane Bilgi Yönetim Sistemi
AHBS: Aile Hekimliği Bilgi Sistemi
LBYS: Laboratuvar Bilgi Yönetim Sistemi
PACS/RIS:Görüntü Saklama ve Arşivleme Sistemleri/Radyoloji Bilgi Sistemi

4. PROSEDÜR METNİ

4.1. Mal ve Hizmet Alımları Güvenliği

4.1.1. Satın alma faaliyetleri; 4734 sayılı Kamu İhale Kanunu, 4735 sayılı Sözleşmeler Kanunu, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, Kamu İhale Kurumu Tebliğleri ve yönetmeliklerinin tanımlamış olduğu usul ve esaslara göre yapılır.

4.1.2. Satın alma faaliyetine konu olan iş kapsamında; yüklenicinin yükümlülüklerini gerçekleştirmesi için yükleniciye özel koruma ihtiyacı olan veri/ bilgi teslim edilmesi, ilgili kurumun fiziki alanlarında personel çalıştırılması veya kurum bilgi sistemlerine (uzaktan erişimler dâhil) erişim yapılması ihtiyacı olması halinde; satın alma için hazırlanan teknik ya da idari şartnamelere "Bilgi Güvenliği Gereksinimleri" başlığı altında asgari olarak aşağıdaki hususlar eklenir:

4.1.2.1. Yüklenici sözleşmeye konu yükümlülüklerini ifa ederken, Bakanlık Bilgi Güvenliği politikalarına uymak

zorundadır. Bakanlığın Bilgi Güvenliği Politikaları, "Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi" ve "Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu"nda açıklanmıştır. Bahse konu dokümanlara, Bakanlığın resmi web sitesinden erişilebilir.

4.1.2.2. Bakanlık/Kurum BGYS Politikaları uyarınca, idareye ait bilgilerin korunması maksadıyla, yükleniciler ile "Kurumsal Gizlilik Sözleşmesi" ve söz konusu iş kapsamında çalışacak olan yüklenici personeli ile "Personel Gizlilik Sözleşmesi" imzalanır. Bahse konu dokümanların boş halleri, hazırlanan teknik veya idari şartnameye eklenir.

4.1.2.3. İhaleyi kazanan firma ile sözleşmenin imzalanmasını takiben kurumdaki yetkili makam (Satın Alma Birimi ve/veya Kurum Bilgi Güvenliği Yetkilisi) huzurunda "Kurumsal Gizlilik Sözleşmesi" imzalanır.

4.1.2.4. "Kurumsal Gizlilik Sözleşmesi" ve ihaleye konu iş kapsamında çalıştırılacak personelin "Personel Gizlilik Sözleşmeleri" imzalanmadan ve idareye teslim edilmeden, yüklenici tarafından işe başlanamaz.

4.1.2.5. Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, "Personel Gizlilik Sözleşmeleri" idareye teslim edildikten sonra tanımlanır.

4.1.2.6. Yapılacak iş kapsamında alt yüklenici kullanılacaksa, alt yükleniciler de yukarıda belirtilen hükümlere aynen uymak zorundadır. Yüklenici, alt yüklenicileri ve çalışanlarının gizlilik sözleşmeleri ile ilgili yükümlüklere uymasından birinci derecede sorumludur.

4.1.3. Kamu kurum ve kuruluşlarınca temin edilecek 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 üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınır.

4.1.3.1. Alınan hizmetle ilgili olarak güvenlik kontrol gereksinimleri, hizmet seviyeleri ve yönetim gereksinimleri,

4.1.3.2. Yükleniciye verilecek veya erişilecek bilgilerin tanımları ile bu bilgilerin sağlanma veya erişim metodları,

4.1.3.3. Yüklenici ile paylaşılacak olan bilgilerin kabul edilebilir kullanım kuralları ve gerekiyorsa kabul edilemez kullanım durumları,

4.1.3.4. Yüklenici personeli için erişim yetkilendirme ve yetki kaldırma prosedürleri,

4.1.3.5. Bilgi güvenliği olay müdahale prosedürleri (özellikle olay bildirimi ve olay müdahalesinde işbirliği kuralları).

4.1.4. "Kurumsal Gizlilik Sözleşmesi" ve "Personel Gizlilik Sözleşmesi" olarak SBSGM tarafından kullanılan ve örneği Kılavuz'un ekinde yer alan sözleşmeler kullanılabilir. Bahse konu sözleşmelerin içeriği, satın almaya konu mal veya hizmetin türüne ve kurumun kendine özgü ihtiyaçlarına bağlı olarak revize edilip kullanılabilir.

4.1.5. Yüklenicinin fikri mülkiyet hakları ve telif hakları dâhil, yasal ve düzenleyici gereksinimlere uyması ile ilgili hususlar satın alma dokümanlarına konulur.

4.1.6. Alınacak mal veya hizmetin tahmini bedelleri bağlamında idare tarafından yapılan yaklaşık maliyet çalışması, ihale aşamasına kadar gizli tutulur.

4.1.7. Söz konusu alım için gerekli iş tanımı ölçütleri, personel istihdam edilecekse ilgili personel özellikleri açıkça belirtilir.

4.1.8. Tedarikçinin çalıştırılacağı personelin adli sicil kayıtlarını sorgulatıp, bunları idareye bildirmesi istenir. Projelerde çalışacak personelin; TCK'nın 53'ncü maddesinde belirtilen süreler geçmiş olsa bile devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan mal varlığı değerlerini aklama ve kaçakçılık suçlarından

mahkûm olmamış olması gerekir.

4.1.9. Satın alma faaliyetine konu iş uygulama/yazılım geliştirme ise; uygulama ile ilgili gerekli dokümantasyonun hazırlanması, ilgili projeye ait kaynak kodların teslim edilmesi gibi hususlar, idare tarafından açıkça tanımlanır. Ayrıca geliştirilen yazılım/uygulamada özel nitelikli kişisel veriler işlenecek ise KVKK'nın 2018/10 sayılı kararında belirtilen ilave güvenlik tedbirleri ile ilgili hususlar da teknik şartnamelere eklenir.

4.1.10. Anlaşmalar gereği, tedarikçilerce üretilen hizmet raporları düzenli olarak gözden geçirilir ve proje ilerleme toplantıları yapılır.

4.1.11. Tedarikçilere verilen fiziksel ve mantıksal erişimler, periyodik olarak gözden geçirilir. Hassasiyet arz eden erişimler için yönetim onayı alınır. Olası güvenlik zafiyetlerinin engellenmesi için yüklenici personeline verilen yetkiler periyodik olarak kontrol edilir. İhtiyacın bitmesi durumunda, verilen yetkiler kaldırılır. Personelin kurumla ilişiği kesilir kesilmez, erişim yetkileri de kapatılır.

4.1.12. Yazılım tedarikçilerinin destek faaliyetleri (ör: tedarikçi personelinin sistem üzerinde çalıştırdığı komutların iz kayıtlarının tutulması ve incelenmesi gibi) izlenir.

4.1.13. Ürünlerin satın alınmadan önce kurumsal olarak belirlenen güvenlik gereksinimleri için risk oluşturmadığından emin olunması için test edilmesi gerekir.

4.2. SBYS Firmaları ile İlişkilerde Dikkat Edilecek Hususlar

4.2.1. Sağlık tesisleri tarafından klinik, idari ya da yönetimsel amaçlarla kullanılan, gerektiğinde diğer bilgi yönetim sistemleri ile veri alış verişi yapabilen yazılım, sistem ya da alt sistemler Sağlık Bilgi Yönetim Sistemi (SBYS) olarak adlandırılır.

4.2.2. Hastane Bilgi Yönetim Sistemi (HBYS), Aile Hekimliği Bilgi Sistemi (AHBS), Laboratuvar Bilgi Yönetim Sistemi (LBYS), Görüntü Saklama ve Arşivleme Sistemleri/Radyoloji Bilgi Sistemi (PACS/RIS) vb. yazılımların tamamı SBYS yazılımıdır.

4.2.3. Taşra birimleri tarafından gerçekleştirilecek SBYS alımlarında, SBSGM tarafından yayımlanan Hastane Bilgi Yönetim Sistemi Alım Kılavuz'unda belirtilen esaslar çerçevesinde hareket edilir.

4.2.4. Sağlık kuruluşlarında kullanılacak tüm SBYS yazılımlarının Bakanlık tarafından yayımlanan sağlık bilişimi standartlarına ve veri gönderim servislerine uyumlu olmaları gerekmektedir. SBYS üreticisi firmalar, Bakanlık tarafından talep edilen geliştirmeleri ve güncellemeleri belirtilen süreler içerisinde sistemlerine yansıtmakla mükelleftir. 154 Bilgi Güvenliği Politikaları Kılavuzu

4.2.5. SBYS yazılımları, sağlık kuruluşları içerisindeki entegre edilebilir cihazlar, sistemler ve Bakanlığın tanımladığı ve yürüttüğü uygulamalarla uyum sağlamak zorundadır.

4.2.6. SBYS yazılım üreticileri, Bakanlık Kayıt Tescil Sistemine (KTS) kayıt olarak akredite olurlar. Üreticilerin KTS'ye kayıt olabilmesi için istenilen sertifikalar ve belgeler ilgili mevzuatta belirtilmiştir.

4.2.7. Bakanlık tarafından istenilen sertifika ve belgeleri teslim eden SBYS yazılım üreticileriyle, KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesi imzalanır ve üretici firma KTS'ye kaydedilir.

4.2.8. KTS'ye kayıt olan SBYS yazılım üreticileri Bakanlık tarafından yayımlanan sağlık bilişimi standartlarına uygunluk açısından denetlenir.

4.2.9. Sağlık bilişimi standartlarına ve ilgili mevzuatlara uyumlu olmayan; bilgi, belge, sertifika ve doküman eksiği olan SBYS yazılım üreticileri, KTS web sayfasında pasif listeye alınır. Eksiği olmayan SBYS yazılım üreticileri ise aktif listede yer alır.

4.2.10. İlgili mevzuat kapsamında SBYS yazılım üreticilerine eksikliklerini gidermeleri için süre verilir. Bu süre içerisinde eksikliklerini gideren SBYS yazılım üreticileri aktif listeye alınır.

4.2.11. Kullanılmasına karar verilen sağlık bilişimi standartları ve veri gönderiminde dikkat edilecek hususlar

SBSGM web sayfasında yayımlanır ve güncellenir.

4.2.12. Sağlık hizmeti sunucularınca SBYS yazılım üreticilerinden, ürettiği SBYS yazılımının minimum şartlara uyum sağladığını gösteren "KTS Kayıt Belgesi" istenir. KTS kayıt belgesinin geçerliliği KTS web sayfası üzerinden sorgulanır.

4.2.13. KTS yetki belgesi olmayan, geçersiz yetki belgesi ibraz eden ya da KTS web sayfasında pasif listede yer alan SBYS yazılım üreticileri ile sözleşme imzalanmaz.

4.2.14. Sağlık kuruluşları ile SBYS yazılım üreticisi arasında yaşanabilecek uyuşmazlıklarda uygulanacak cezai şartların SBYS yazılım üreticisi ile yapılacak sözleşmelerde yer alması sağlanır.

4.2.15. Sağlık kuruluşları ve aile hekimleri, SBYS yazılım üreticisi ve bayileriyle ayrıca gizlilik sözleşmesi imzalamalıdır. Sağlık tesisleri ve aile hekimleri bu maksatla KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesini kullanabilecekleri gibi kendileri de sözleşme metinlerini oluşturabilirler.

4.2.16. SBYS'lerin ilk kurulumu esnasında uzaktan destek ile kurulum talepleri kabul edilmez.

4.2.17. SBYS yazılım üreticisi, ilk kurulum esnasında çalıştıracağı personel ile ilgili planlamayı kurulum ve proje planında detaylı olarak açıklamak zorundadır.

4.2.18. Kurulum ve proje planının işletmeye alınacağı tarihe, sağlık kuruluşları tarafından karar verilir. Sözleşme imzalandıktan sonra SBYS'nin işletmeye alınacağı tarih, sağlık kuruluşları tarafından hazırlanan şartnamelerde belirtilir.

4.2.19. Sağlık kuruluşları, HBYS tedarikçilerinden en az altı ayda bir kez olacak şekilde son alınan yedek üzerinden veri kurtarma testi yapmasını istemeli ve gerekli kontrolleri yapmalıdır.

4.2.20. Herhangi bir sebeple mevcut SBYS yazılımının kullanımına son verilirse, verilerin tamamı (orijinal veri tabanı formatında) ve VEM görüntüleri kolay ve sorunsuz okunabilir bir medya ortamında, 3 (üç) kopya halinde sağlık kuruluşuna teslim edilmek zorundadır

4.2.21. Kritik alanlardaki değiştirme ve silme işlemlerinin, ancak yetki ölçüsünde yapılması gerekir. Değişikliklere sonradan erişim ve geri düzeltme için mutlaka iz kaydı dosyaları detayları olarak tutulmalı veya VTYS katmanındaki denetleme (audit) uygulama yazılımından da desteklenir olmalıdır

4.2.22. Kişisel sağlık verileri özel nitelikli kişisel veriler kapsamında olması sebebiyle; sözleşme süresince veya sonrasında kayıtlı tüm veriler hiçbir surette, hiçbir zaman SBYS üreticisinde kalmak üzere kopyalanamaz, çıktı alınamaz, firma sunucularına aktarılamaz, ifşa edilemez.

4.2.23. SBYS yazılımları tüm sistem genelindeki kullanıcı, işlem ve bilgi düzeylerinde bilgi gizliliğini ve güvenliğini sağlamak zorundadır. Her kullanıcının gerektiğinde değiştirilebilir kişisel bir parolası olmalıdır. Bu parola ile farklı bir lokasyonda oturum açıldığında ilk oturum otomatik olarak kapatılmalıdır. Bir kişiye ait parolanın birden çok kişi tarafından kullanılmasına izin verilmemelidir

4.2.24. Çeşitli yetki düzeyleri ve grupları tanımlanabilmeli, yetki değişimi SBYS Yöneticisi tarafından yapılabilmelidir. Verilere erişim bu tanımlamalar çerçevesinde yapılmalıdır.

4.2.25. SBYS'de kullanıcılar için saat bazında sisteme giriş sınırlandırması yapılabilmelidir.

4.2.26. SBYS'de kullanıcıların otomasyona giriş-çıkış zamanları ve geçersiz giriş denemeleri istenildiğinde raporlanabilmelidir.

4.2.27. Poliklinik, Klinik, Laboratuvar bazında yetkilendirmeler yapılabilmelidir. Kullanıcının yetki verilmeyen bir poliklinikteki hasta listesine erişimi engellenmelidir

4.2.28. SBYS yazılımlarında Kılavuz'un 6.3 (Parola Güvenliği) maddesinde belirtilen parola özellikleri tanımlanabilmeli ve bu kurala uymayan parolalar kabul edilmemelidir.

4.2.29. Sağlık kuruluşu ile ilişiği kalıcı olarak kesilen tüm personelin SBYS erişim yetkisi tamamen ve otomatik olarak iptal edilmelidir.

4.2.30. Geçici olarak sağlık kuruluşunda bulunmayan (izin, rapor, geçici görev kurs, eğitim vb.) personelin SBYS'ye girişi otomatik olarak engellenmelidir

4.2.31. Sunucu işletim sistemi, sunucu yazılımları, veri tabanında yapılacak yapısal değişiklikler gibi tüm sistemi etkileyen güncellemeler mesai saatleri dışında veya hasta yoğunluğunun en az olduğu saatlerde yapılmalıdır. Acil müdahale edilmesi gereken bir arıza durumunda ise mesai saatleri içinde güncelleme yapılabilir.

5. İLGİLİ DOKÜMANLAR

- **Kurumsal Gizlilik Sözleşmesi**
- **Personel Gizlilik Sözleşmesi**
- **Kurumsal Gizlilik Taahhütnamesi**

6. SORUMLULAR

T.C Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesislerinde bünyesinde görev yapan tüm personel (kamu personeli, tam zamanlı ya da yarı zamanlı olarak çalışan sözleşmeli personel, yüklenici firma çalışanları, iş ortaklarının çalışanları, destek alınan firmaların personeli vb.) ve T.C Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesisleri ile herhangi bir satın alma işlemi kapsamında yüklenici olarak işlem yapan tüm gerçek ve tüzel kişiler sorumludur.

Hazırlayan	Kontrol Eden	Onaylayan
Oğuz KARABAĞ Bilgi Güvenliği Yetkilisi	Uz. Dr. Nejat AKIN Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Op. Dr. Erkan ÖZDEMİR İl Sağlık Müdürü