1. AMAÇ

Bu politikanın amacı **T.C. Sağlık Bakanlığı Burdur İl Sağlık Müdürlüğü ve bağlı birimleri/tesisleri** için Mal ve Hizmet Alımları sırasında Bilgi Güvenliği hususundaki uyulacak kurallar ile varlık sahibi ve çalışan tüm personelin görev ve sorumluluklarını belirlemektir.

1. KAPSAM

T.C. Sağlık Bakanlığı Burdur İl Sağlık Müdürlüğü ve bağlı birimleri/tesisleri dâhilindeki Tedarikçi, Hizmet Sunucusu, yapım Müteahhidi ve Yüklenici ile bunlar aracılığı ile iş veya hizmet görenler ile mal ve hizmet alımları süreçlerindeki tüm unsurları kapsamaktadır.

1. POLİTİKA METNİ
   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.
   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:
2. Yüklenici sözleşmeye konu yükümlülüklerini ifa ederken, Kurum Bilgi Güvenliği politikalarına uymak zorundadır. Kurumun Bilgi Güvenliği Politikalarına Burdur İl Sağlık Müdürlüğünün resmi web sitesinde bulunan “Bilgi Güvenliği” başlığı altından erişilebilir.
3. Bakanlık/Kurum BGYS Politikaları uyarınca, idareye ait bilgilerin korunması maksadıyla, yükleniciler ile “Kurumsal Gizlilik Taahhütnamesi” ve söz konusu iş kapsamında çalışacak olan yüklenici personeli ile “Personel Gizlilik Sözleşmesi” imzalanır. Bahse konu dokümanların boş halleri, hazırlanan teknik şartname, sözleşme taslağı veya idari şartnameye ek olarak eklenir.
4. İhaleyi kazanan firma ile sözleşmenin imzalanmasını takiben kurumdaki yetkili makam (Satın Alma Birimi ve/veya Kurum Bilgi Güvenliği Yetkilisi) huzurunda “Kurumsal Gizlilik Taahhütnamesi” imzalanır.
5. “Kurumsal Gizlilik Taahhütnamesi” ve ihaleye konu iş kapsamında çalıştırılacak personelin “Personel Gizlilik Sözleşmeleri” imzalanmadan ve idareye teslim edilmeden, yüklenici tarafından işe başlanamaz.
6. Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, “Personel Gizlilik Sözleşmeleri” ve “Uzaktan Erişim Sözleşmesi” imzalanıp idareye teslim edildikten sonra tanımlanır.
7. 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. Tüm Alt yükleniciler için de üstte belirtilen maddeler geçerlidir.
   1. Yukarıda belirtilen gereksinimlere ek olarak, aşağıdaki konular teknik/idari şartnamelere veya tedarikçiler ile imzalanacak gizlilik sözleşmelerine eklenerek, garanti altına alınır:
8. Alınan hizmetle ilgili olarak güvenlik kontrol gereksinimleri, hizmet seviyeleri ve yönetim gereksinimleri,
9. Yükleniciye verilecek veya erişilecek bilgilerin tanımları ile bu bilgilerin sağlanma veya erişim metodları,
10. Yüklenici ile paylaşılacak olan bilgilerin kabul edilebilir kullanım kuralları ve gerekiyorsa kabul edilemez kullanım durumları, Yüklenici personeli için erişim yetkilendirme ve yetki kaldırma prosedürleri,
11. Bilgi güvenliği olay müdahale prosedürleri (özellikle olay bildirimi ve olay müdahalesinde işbirliği kuralları).
    1. Yüklenicinin fikri mülkiyet hakları ve telif hakları dâhil, yasal ve düzenleyici gereksinimlere uyması ile ilgili hususlar satın alma dokümanlarına konulur.
    2. Alınacak mal veya hizmetin tahmini bedelleri bağlamında idare tarafından yapılan yaklaşık maliyet çalışması, ihale aşamasına kadar gizli tutulur.
    3. Söz konusu alım için gerekli iş tanımı ölçütleri, personel istihdam edilecekse ilgili personel özellikleri açıkça belirtilir.
    4. 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.
    5. 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.
    6. Anlaşmalar gereği, tedarikçilerce üretilen hizmet raporları düzenli olarak gözden geçirilir ve proje ilerleme toplantıları yapılır.
    7. Tedarikçilere verilen fiziksel ve mantıksal erişimler, kurumların bilgi güvenliği alt komisyonlarında 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.
    8. Yazılım tedarikçilerinin destek faaliyetleri (ör: tedarikçi personelinin sistem üzerinde çalıştırdığı komutların iz kayıtlarının tutulması ve incelenmesi gibi) izlenir.
    9. Ürünlerin satın alınmadan önce kurumsal olarak belirlenen güvenlik gereksinimleri için risk oluşturmadığından emin olunması için test edilmesi gerekir.
    10. SBYS Firmaları ile İlişkilerde ve Teknik Şartname hazırlanırken aşağıdaki belirtilen ve BGYS ile doğrudan ilgili olan Hususlara Dikkat Edilir:
12. 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.
13. 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.
14. 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.
15. SBYS yazılımları, sağlık kuruluşları içerisindeki entegre edilebilir cihazlar, sistemler ve Bakanlığın tanımladığı ve yürüttüğü uygulamalarla uyum sağlamak zorundadır.
16. SBYS yazılım üreticilerinin, Bakanlık Kayıt Tescil Sisteminde (KTS) kayıtlı olup akreditasyonlarını tamamlamış olmaları gerekmektedir. Üreticilerin KTS’ye kayıt olabilmesi için istenilen sertifikalar ve belgeler ilgili mevzuatta belirtilmiştir.
17. SBYS yazılım üreticileriyle “Kurumsal Gizlilik Taahhütnamesi”, SBYS Personeli ile de “Personel Gizlilik Sözleşmesi” imzalanır.
18. Sağlık bilişimi standartlarına ve ilgili mevzuatlara uyumlu olmayan; bilgi, belge, sertifika ve doküman eksiği olan SBYS yazılım üreticileri, Bakanlığımız KTS web sayfasında pasif listeye alındığından bu üreticilerle herhangi bir anlaşma veya sözleşme yapılamaz.
19. Kullanılmasına karar verilen sağlık bilişimi standartları ve veri gönderiminde dikkat edilecek hususlar SBSGM web sayfasında yayımlanır ve güncellenir. Üreticiler tüm bu güncellemeleri takip etmek ve bunları sağlık tesislerinde ilgili yasalar ve mevzuatlar çerçevesinde uygulamakla yükümlüdür.
20. Sağlık kuruluşları ile SBYS yazılım üreticisi arasında yaşanabilecek uyuşmazlıklarda uygulanacak cezai şartların SBYS yazılım üreticisi ile yapılacak sözleşmelerde yer alması sağlanır.
21. Sağlık kuruluşları ve Aile Hekimleri, SBYS yazılım üreticisi ve bayileriyle ayrıca gizlilik sözleşmesi imzalamalıdır. Sağlık Tesisleri ve Aile Hekimleri bu maksatla Müdürlüğümüz web sitesinde yayımlanan “Bilgi Güvenliği” başlığı altındaki “Kurumsal Gizlilik Taahhütnamesini” kullanabilecekleri gibi kendileri de sözleşme metinlerini oluşturabilirler.
22. SBYS’lerin ilk kurulumu esnasında uzaktan destek ile kurulum talepleri kabul edilmez.
23. SBYS yazılım üreticisi, ilk kurulum, eğitimler ve ilgili şartnamede belirtilen diğer iş ve işlemler sırasında çalıştıracağı personel ile ilgili planlamayı şartnamede belirtildiği şekilde planlamak ve yerine getirmek zorundadır.
24. Kurulum ve proje planının işletmeye alınacağı tarihe, sağlık kuruluşları tarafından karar verilir. Sözleşme imzalandıktan sonra SBYS’nin işletmeye alınacağı tarih, İdare tarafından hazırlanan şartnamelerde belirtilir.
25. 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.
26. Herhangi bir sebeple mevcut SBYS yazılımının kullanımına son verilirse, verilerin tamamı orijinal veri tabanı formatında, kolay ve sorunsuz okunabilir bir medya ortamında, 3 (üç) kopya halinde sağlık kuruluşuna teslim edilmek zorundadır.
27. 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.
28. 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.
29. 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.
30. Çeşitli yetki düzeyleri ve grupları tanımlanabilmeli, yetki değişimi SBYS Yöneticisi tarafından yapılabilmelidir. Verilere erişim bu tanımlamalar çerçevesinde yapılmalıdır.
31. SBYS’de kullanıcılar için saat bazında sisteme giriş sınırlandırması yapılabilmelidir.
32. SBYS’de kullanıcıların otomasyona giriş-çıkış zamanları ve geçersiz giriş denemeleri istenildiğinde raporlanabilmelidir.
33. Poliklinik, Klinik, Laboratuvar bazında yetkilendirmeler yapılabilmelidir. Kullanıcının yetki verilmeyen bir poliklinikteki hasta listesine erişimi engellenmelidir.
34. SBYS yazılımlarında Müdürlüğümüzün PAROLA GÜVENLİĞİ POLİTİKASI’nda belirtilen parola özellikleri tanımlanabilmeli ve bu kurala uymayan parolalar kabul edilmemelidir.
35. Sağlık kuruluşu ile ilişiği kalıcı olarak kesilen tüm personelin SBYS erişim yetkisi tamamen ve otomatik olarak iptal edilmelidir.
36. Geçici olarak sağlık kuruluşunda bulunmayan (izin, rapor, geçici görev kurs, eğitim vb.) personelin SBYS’ye girişi otomatik olarak engellenmelidir.
37. 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 şartnamede belirtildiği şekilde mesai saatleri içinde güncelleme yapılabilir.
    1. Varlık emanetçisi ya da kullanıcısı olan yüklenici veya personel, kendisine teslim edilen varlıkları korumak, iade durumunda ise sağlam ve eksiksiz teslim etmekle yükümlüdür.
    2. Tedarikçi, Hizmet Sunucusu, Yapım Müteahhidi, Yüklenici ve personeli de dâhil olmak üzere üçüncü şahısların, mal hizmet alımları için ihale dokümanlarının hazırlandığı ve ihale hazırlıklarının yapıldığı alanlarda bulunmaları yasaktır.
    3. İhale hazırlıklarının yapıldığı alanların giriş-çıkış kapıları kamera ile kayıt altına alınmalı ve kayıtlar kanunda belirtildiği süreyle muhafaza edilmelidir.
    4. İhale hazırlıklarının yapıldığı bilgisayarlar, kurum dışından ve kurumun ağındaki diğer bilgisayarlardan erişime kapalı olmalıdır.
    5. İhale hazırlıklarının yapıldığı alanlarda görünür yerlere BGYS Temiz Masa Temiz Ekran Politikasını içeren doküman asılmalıdır.
    6. İhale bilgilerini içeren bilgi ve belgelerin gizliliğini ihlal edenler hakkında ilgili mevzuat hükümleri çerçevesinde cezai yaptırımlar uygulanır.
    7. İhale ile ilgili kullanılan bilgi sistemleri parola korumalı olmalı, kullanılan parolalar kurum BGYS Politika ve Prosedürlerine uygun olarak oluşturulmalıdır.
    8. İhale hazırlıklarının yapıldığı bilgisayarlara varlık sahibi veya varlık emanetçisinin gözetiminde ve nezaretinde teknik destek verilecektir.
    9. Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde yapılır. Gerektiğinde anlaşmalar yenilenir ve güncellenir.
    10. Bu Politika metni yayımlandığı tarihten itibaren yürürlüğe girer ve bu politika metninin 2. Maddesinde bulunan kapsamda belirtilen tüm Kurumlar, Üreticiler ve personel bu politika metnine uymakla yükümlüdürler.