Genel Hususlar:

1. Bu liste, BG.PO.22 Tedarikçi İlişkilerinde Bilgi Güvenliği Politikası uyarınca Genel Müdürlüğümüz tarafından yapılacak tedarik işlemlerinde, ilgili dokümanlara bilgi güvenliği ile ilgili gereksinimlerin eksiksiz olarak girilmesini sağlamak maksadıyla bir rehber olarak hazırlanmıştır.

2. Sözleşmeye konu iş kapsamında;

   a. Firma/firma personeli tarafından "**kuruma ait gizli kalması gereken bilgilere veya kurum bilgi işleme tesislerine (personel çalışma alanlarına, veri merkezine, veri tabanlarına, sunuculara vb.) yüklenici tarafından fiziksel olarak veya uzaktan erişim yöntemleriyle erişim sağlanacak**" ise veya,

   b. Firma/firma personeline "**kuruma ait gizli kalması gereken bilgilerin teslim edilecek olması**" halinde,

Aşağıdaki listede yer alan maddelerden (proje makamları/ihtiyaç sahibi makamlar tarafından) uygun görülenler, teknik şartnamelere ve/veya idari şartnamelerin diğer hususlar bölümüne yazılır.

3. Hiçbir erişim ihtiyacının söz konusu olmadığı, **depoya (veya kullanıcıya) doğrudan teslim şeklinde yapılan mal ve hizmet alımları ile gizlilik dereceli bilgi işlenmeyen eğitim ve çalıştay hizmetleri** teknik şartnamelerinde, özel olarak **bilgi güvenliği gereksinimlerinin listelenmesine gerek bulunmamaktadır**.

4. Teknik şartnamelere eklenmesi uygun görülen bilgi güvenliği gereksinimleri, tedarik faaliyetinin türüne bağlı olarak aşağıdaki tabloda ayrıntılı olarak listelenmiştir.

S.Nu.	Bilgi Güvenliği Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
1	Yüklenici sözleşmeye konu yükümlülüklerini yaparken, Bakanlık bilgi güvenliği politikalarına uymak zorundadır. Bakanlığın bilgi güvenliği politikaları, Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunda açıklanmıştır. Bahse konu dokümanlara, Genel Müdürlük web sitesi mevzuat bölümü veya bilgi güvenliği web sitesinden erişim sağlanır.	√	√

S.Nu.	Bilgi Güvenliği Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
2	Yüklenicinin herhangi bir iş ve işleminde veya yükümlü olduğu iş ve sistemle ilgili olarak Bakanlık bilgi güvenliği politikalarına aykırı hareket etmesi halinde, bu durum İdare tarafından yazılı olarak yükleniciye bildirilir ve gerekli düzenlemeleri yapması istenir. Yükleniciye bu tarzda bir bildirim yapılmamış olması halinde, yüklenicinin bilgi güvenliği politikalarına uyduğu kabul edilir.	√	√
3	Sağlık Bilgi Sistemleri Genel Müdürlüğü BGYS Politikaları uyarınca, idareye ait bilgilerin korunması maksadıyla, yükleniciler ile BG.SZ.02 Kurumsal Gizlilik Taahhütnamesi ve söz konusu iş kapsamında çalışacak olan yüklenici personeli ile BG.SZ.01 Personel Gizlilik Sözleşmesi imzalanır. Bahse konu dokümanlara, Genel Müdürlük bilgi güvenliği web sitesinden erişim sağlanır.	√	√
4	Sözleşmeye konu iş kapsamında alt yüklenici kullanılacaksa, ana yüklenici tarafından tüm alt yüklenicilere BG.SZ.02 Kurumsal Gizlilik Taahhütnamesi imzalatılır ve taahhütnamelerin bir sureti idareye teslim edilir. Aynı şekilde alt yüklenici çalışanları ile de BG.SZ.01 Personel Gizlilik Sözleşmesi imzalanır. Alt yükleniciler ve çalışanlarına ait sözleşmeler İdareye teslim edilmeden, alt yükleniciler çalışmalara katılamaz. Alt yükleniciler ile BG.SZ.02 Kurumsal Gizlilik Taahhütnamesi imzalanması, asıl yüklenicinin gizlilik ile ilgili sorumluluklarını ortadan kaldırmaz veya değiştirmez.	√ (1)	√ (1)
5	BG.SZ.02 Kurumsal Gizlilik Taahhütnamesi ve ihaleye konu iş kapsamında çalıştırılacak anahtar personelin BG.SZ.01 Kişisel Gizlilik Sözleşmelerinin imza işlemleri tamamlanmadan, yüklenici tarafından işe başlanamaz.	√	√
6	Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, BG.SZ.01 Kişisel Gizlilik Sözleşmeleri idareye teslim edildikten sonra tanımlanır.	√	√
7	Yüklenici personelinin Bakanlık bilişim kaynaklarına erişimi, İdare tarafından sağlanan VPN hizmeti üzerinden yapılır. VPN erişimi yapılabilmesi için BG.SZ.02 Kurumsal Gizlilik Taahhütnamesi ve BG.SZ.01 Personel Gizlilik Sözleşmelerinin idareye teslim edilmiş olması gerekir.	√ (2)	√ (2)

S.Nu.	Bilgi Güvenliği Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
8	Yüklenici, çalıştırılacağı personelin adli sicil kayıtlarını sorgulatıp, bunları idareye bildirir. Çalışanların 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.	√	√
9	Yüklenicinin (ve alt yüklenicilerin) işe başlama tarihi itibarı ile geçerli olan TÜRKAK onaylı bir belgelendirme kuruluşu tarafından verilmiş ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) Sertifikası olması gerekir.		√ (3)
10	Yüklenicinin proje kapsamında kullanacağı bilgisayarlarda yer alan idareye ait veriler (yazılım kaynak kodları dâhil), Bakanlık bilgi güvenliği politikaları uyarınca şifreli olarak muhafaza edilir.		√
11	Projede kullanılan bilgisayarların herhangi bir nedenle kullanımdan çıkarılması durumunda, ilgili bilgisayarlar güvenli silme işlemine tabi tutulur ve bununla ilgili tutanaklar idareye teslim edilir.		√
12	Yüklenici [PROJE VEYA SİSTEMİN ADI]'in işletim ve destek faaliyetleri esnasında 6698 sayılı Kişisel Verilerin Korunması Kanununda belirtilen "VERİ İŞLEYEN" sıfatıyla hareket eder.		√ (4)
13	Yüklenici, verilerin işlenmesi esnasında veri güvenliğinin sağlanması, erişim ve yetkilendirme gibi konularda tereddütte kalması durumunda, en seri yöntem ile İdareye başvurur ve İdarenin vereceği talimatlar doğrultusunda hareket eder.		√
14	Sistemde işlenen özel nitelikli kişisel verilerin güvenliği için, Kişisel Verileri Koruma Kurulunun 31 Ocak 2018 tarihli, 2018/10 sayılı Kararında belirtilen önlemler alınır.		√ (5) (6)

S.Nu.	Bilgi Güvenliği Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
15	Kullanıcıların web tabanlı uygulamalara giriş arayüzleri için güvenlik kodu (captcha) uygulaması yapılır. Bakanlık kullanıcıları ve vatandaşlar tarafından giriş yapılan arayüzler için farklı captcha uygulaması istenebilir.		√
16	Parola ile giriş gerektiren tüm uygulamaların, Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunda belirtilen parola politikası ile uyumlu olması sağlanır. Doğrudan vatandaşlar tarafından giriş yapılan uygulamalar için farklı parola politikası uygulanabilir.		√
17	Parola değişimi yapılan tüm ekranlarda parola değişimi öncesinde, kullanıcı kimliğinin doğrulanması (eski parolanın girilmesi, SMS veya e-posta ile doğrulama vb. yöntemlerle) sağlanır.		√
18	Yönetici ve son kullanıcılar tarafından açılan oturumlar için zaman aşımı (time out) süreleri belirlenebilmelidir. Bu sürelerin parametrik olarak değiştirilmesi için gerekli yönetim arayüzleri sağlanır.		√
19	Sisteme oturum açıldığında, kullanıcılara en son yapılan başarılı oturum açma zamanı gösterilir ve başarısız oturum açma girişmeleri hakkında bilgi verilir.		√
20	Tüm parolalar şifreli (özetlenmiş) olarak saklanır. Şifreleme (özetleme) işlemleri için Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunda belirtilen özetleme algoritmaları ve anahtar boyu değerleri kullanılır.		√
21	Sistem yönetimi maksatlı olarak sunucu/uygulamalara yapılacak erişimlerde, erişim yapan kullanıcılara sorumluluklarını açıklayan bir karşılama mesajı (onam metni) konulur.		√
22	Veri tabanında saklanan verilerin yetkisiz kişiler tarafından görüntülenmesini engellemek maksadıyla, İDARE ile ortak olarak yapılacak çalışma sonucunda tespit edilen veri alanları, veri tabanında maskelenmiş (data masking) ve/veya şifreli olarak saklanır.		√

S.Nu.	Bilgi Güvenliği Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
23	Kullanıcı arayüzleri ve raporlarda bir bütün olarak görüntülenme ihtiyacı olmayan kişisel veri alanları için veri maskeleme (data masking) işlemi yapılır. Hangi alanların maskeleneceği İDARE ile ortak olarak yapılacak çalışma ile belirlenir.		√
24	Hassas bilgiler (TC Kimlik No, Kullanıcı Adı, Parola, Token vb.) hiçbir şekilde URL'ler içinde açık olarak taşınmaz.		√
25	Web arayüzleri ile erişilen tüm uygulamalara HTTPS protokolü kullanılarak erişilir. Bu maksatla ihtiyaç duyulan SSL sertifikaları İDARE tarafından sağlanır.		√
26	Sistemi oluşturan bileşenler arasında veya dış sistemler ile entegrasyon kapsamında gerçekleşen her türlü veri aktarımı/değişimi işlemleri şifrelenmiş olarak gerçekleştirilir.		√
27	Yazılımlara ait kaynak kodları İdare tarafından sağlanan Kaynak Kod Yönetim Aracında saklanır.		√
28	Tüm geliştirme işlemleri gerçek (canlı) ortamdan farklı bir ortamda yapılır. Bu maksatla tesis edilecek yazılım geliştirme ortamı için ihtiyaç duyulan yazılım ve donanımlar [İDARE ve/veya YÜKLENİCİ] tarafından sağlanır. Geliştirilen yazılımların test edilmesi için gerçek ortam verileri kullanılmaz.		√
29	Yazılım geliştirme esnasında, güvenli yazılım geliştirme pratikleri uygulanır. Bu amaçla İDARE tarafından hazırlanan BG.Lİ.21 GÜVENLİ YAZILIM GELİŞTİRME KONTROL LİSTESİ kullanılır. Güncel listeye Genel Müdürlüğün bilgi güvenliği web sitesinden erişim sağlanır.		√
30	Güvenli Yazılım Geliştirme Kontrol Listesinde yer alan kontrollerden PROJE'de uygulanması teknik nedenlerle mümkün olmayan maddeler, İDARE ve YÜKLENİCİ tarafından müşterek olarak belirlenir.		√

S.Nu.	Bilgi Güvenliği Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
31	İDARE gerekli gördüğü durumlarda kendi personeline ve/veya üçüncü kişi ve/veya firmalara güvenlik testleri yaptırabilir. Güvenlik testleri SİSTEM'in güvenlik açıklarına karşı taranmasını, analiz edilmesini, raporlanmasını ve doğrulama testlerini kapsar.		√
32	Güvenlik testlerinde tespit edilen güvenlik açıklarından proje ile ilgili olanlar YÜKLENİCİ tarafından düzeltilir. İDARE'nin ağ altyapısı, donanım yapılandırması vb. sebeplerle İDARE'den kaynaklanan güvenlik açıklarının düzeltilmesinden ve bu açıkların sistemlerde sebep olacağı gecikmelerden/kesintilerden YÜKLENİCİ sorumlu tutulamaz.		√
33	Güvenlik açıklarının çözümlendiğinin YÜKLENİCİ tarafından bildirilmesi sonrası İDARE doğrulama amaçlı olarak güvenlik testi yaptırılabilir. Tekrar edilen testlerde çıkan güvenlik açıkları, YÜKLENİCİ tarafından düzeltilir.		√
34	İDARE, istemesi halinde kendi personeline ve/veya üçüncü kişi ve/veya firmaya kaynak kod analizi yaptırabilir. Analiz işlemleri esnasında talep edilmesi halinde YÜKLENİCİ tarafından analiz yapan kişi veya firmaya destek verilir. Kaynak kod analizleri sonucunda tespit edilen hususlara YÜKLENİCİ tarafından yapılması gereken hususlar, YÜKLENİCİ ve İDARE'nin ortak mutabakatı ile belirlenir.		√
35	Kullanıcılar tarafından yapılan başarılı ve başarısız oturum girişlerine ait iz bilgileri; uygulama tarafından üretilen hata mesajlarına ait iz bilgileri (hata kodu, hata açıklaması, kullanıcı adı, modül, işlem zamanı) iz bilgileri, kullanıcıların hangi tarihte (saat, dakika, saniye bazında), hangi IP adresi ve hangi bilgisayardan sisteme giriş yaptığı bilgileri; iç ve dış paydaşlar için oluşturulan web servislerine ilişkin iz bilgileri ve İDARE'nin belirleyeceği kritik seviyedeki diğer işlemlere ait iz bilgileri kayıt altına alınır.		√
36	Alınan iz bilgileri, bütünlüğü garanti edilecek şekilde etiketlenir ve saklanır.		√

S.Nu.	Bilgi Güvenliği Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
37	Yetkili kullanıcıların iz bilgilerine erişimi, sorgulaması ve raporlaması için ihtiyaç duyulan arayüzler sağlanır.		√
38	Yazılımların yeni sürümleri, test işlemleri tamamlanmadan ve İDARE'nin yazılı onayı alınmadan canlı ortama aktarılmaz. Canlı ortama aktarım öncesinde YÜKLENİCİ tarafından acil durum senaryolarını da içerecek şekilde kurulum (deployment) planları hazırlanır, hazırlanan planlar test edilerek planın uygulanabilir olduğunun teyit edilir, sonrasında canlı ortama kurulum yapılır.		√
39	2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi'nin 12. Maddesi uyarınca; tedarik edilecek yazılım, donanım ve cihaz/sistemlerde mevcut güvenlik önlemlerini aşarak erişim sağlamak üzere özel olarak tasarlanan ve/veya kasıtlı olarak dâhil edilmiş boşluklar veya güvenlik açıkları bulunmadığı konusunda BG.SZ.06 "Arka Kapı Taahhütnamesi" alınır. Arka Kapı Taahhütnamesi öncelikle üretici, üreticiden alınamıyorsa dağıtıcı, her ikisinden de alınamıyorsa yüklenici tarafından imzalanır. Arka Kapı Taahhütnamesi, taahhütnameyi imzalayacak tedarik zinciri bileşeni dikkate alınarak (üretici, dağıtıcı, yüklenici) her bir ürün için ayrı ayrı, (ürünlerin tür, tip, kullanım amacı, marka, model vb. özelliklerine göre gruplandırılarak) her bir grup için ayrı ayrı veya tüm ürünler için tek bir taahhütname olacak şekilde verilebilir.	√ (7)	√ (7)

S.Nu.	Bilgi Güvenliği Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
40	İhaleye konu iş kapsamında yüklenici tarafından işletme, bakım ve idame desteği sağlanacak ise ilgili ihale dokümanlarına mutlaka arıza türleri ve bu arızalara müdahale ve sorun giderme süreleri (SLA: Service Level Agreement) ve bu sürelere uyulmaması halinde uygulanacak cezai yaptırımlar eklenir. Aşağıda örnek bir SLA ifadesi yazılmış olup yazılmış olan seviye ve süreler; işletme, bakım ve idame desteği verilecek PROJE/SİSTEM'in özelliğine bağlı olarak proje makamları tarafından değiştirilebilir veya ayrıntılandırılabilir. **Arıza Türleri ve SLA Süreleri (ÖRNEKTİR)** • SEVİYE I : Kritik Arıza, ilgili sistemin çalışmaması, açılmaması, cevap vermemesi veya çalışması ancak ana işlevlerini yerine getirmesine engel olabilecek veya durmasına yol açabilecek arızalardır. • SEVİYE II : Orta Seviyede Kritik Arıza, ilgili sistemin herhangi fonksiyonun çalışamaz hale gelmesi veya bazı fonksiyonlarının doğru çalışmaması ya da bu nedenle kullanıcıların bu fonksiyonlarını kullanamamalarına yol açan arızalardır. • SEVİYE III : Kritik Olmayan Arıza, SİSTEM'in tüm bileşenlerinde performans sorunlarından kaynaklanan arızalardır. • Oluşan bir arızanın türü konusunda İdare ve YÜKLENİCİ'nin mutabık kalamadığı durumlarda, İDARE'nin belirlediği Üniversite ve/veya TÜBİTAK gibi kurumların görüşüne başvurulur. Bu sürecin tüm masrafları, sorumluluğu tespit edilen tarafça karşılanır. • YÜKLENİCİ, aşağıda temel şartları belirtilen SLA sürelerine göre müdahale ve çözüm gerçekleştirecektir.		√

Arıza Tipi	Müdahale Süresi (Saat)	Arıza Giderme Süresi (Saat)
Seviye I	4	16
Seviye II	8	24
Seviye III	24	72
Arıza giderme süreleri, müdahale sürelerinin tamamlanmasından sonra		

Açıklamalar:

(1) Sözleşmeye konu iş kapsamında alt yüklenici kullanımına müsaade edildiği durumlarda, bu madde yazılacaktır.

(2) Kurulum bilişim kaynaklarına uzaktan erişim yapılması ihtiyacı yok ise bu madde yazılmayacaktır.

(3) İhaleye konu iş için serbest rekabet ortamını bozmayacağının değerlendirildiği durumlarda, bu maddenin yazılması tavsiye edilmektedir.

(4) İhaleye konu iş kapsamında kişisel verilerin işlenmesi söz konusu olduğu durumlarda yazılacaktır.

(5) Özel nitelikli kişisel verilerin işlendiği sistemler için geçerlidir.

(6) Bu maddede yazan hususların yapılması yasal uyumluklar açısından gereklidir. Ancak yoğun olarak özel nitelikli kişisel veri işlenen sistemlerde bu maddenin istenmesi durumunda, başta performans olmak üzere çok ciddi yan etkiler olabilecektir. Proje/sistemde kullanılan/kullanılması planlanan yazılım geliştirme araçları/platformlar ve VTYS yazılımları bu isteği gerçekleştirmek için gereken fonksiyonları desteklemeyebilir. Bu gibi sebeplerle, bu maddenin gereklerinin yapılabilmesi için ciddi yatırımlar yapılmasına ihtiyaç duyulabilir. Bu maddenin şartnameye yazılması halinde olası etkilerinin Proje Yönetimi ekipleri/ihtiyaç sahibi birimlerce ayrıntılı olarak analiz edilerek tespit edilen hususların üst yönetime aktarılması, yazılıp yazılmayacağı konusunda üst yönetimin de katılımı ile bir karar verilmesinin uygun olacağı değerlendirilmektedir.

(7) Mal ve hizmet alımı kapsamında uygulama yazılımı, donanım, işletim sistemi veya bu bileşenlerin bir ya da birkaçını üzerinde barındıran cihaz/sistem tedarik edilecek ise yazılır.