T.C.
SAĞLIK BAKANLIĞI
ARDAHAN İL SAĞLIK MÜDÜRLÜĞÜ
Teknik Şartnameler İçin Bilgi Güvenliği Gereksinimleri Listesi

Kodu	Yayın Tarihi	Revizyon No	Revizyon Tarihi	Sayfa Sayısı / Num.
BY.YD.02	06.11.2018	1	03.07.2019	1/7

S.Nu.	Bilgi Güvenliği Gereksinimi	Açıklamalar
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.	(1)
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.	(1)
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.	(1)
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), (2)
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.	(1)
6	Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, BG.SZ.01 Kişisel Gizlilik Sözleşmeleri idareye teslim edildikten sonra tanımlanır.	(1)

S.Nu.	Bilgi Güvenliği Gereksinimi	Açıklamalar
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.	(3)
8	Tedarik edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik veya arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğini dair üretici ve/veya tedarikçilerden taahhütname alınır.	(11)
9	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.	(1)
10	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.	(4)
11	Yüklenicinin proje kapsamında kullanacağı bilgisayarlarda yer alan idareye ait veriler (yazılım kaynak kodları dâhil), Bakanlık bilgi güvenliği politikaları uyarınca şifreli olarak muhafaza edilir.	(5)
12	Projede kullanılan bilgisayarların herhangi bir nedenle kullanımdan çıkarılması durumunda, ilgili bilgisayarlar güvenli silme işlemine tabi tutulur ve bununla ilgili tutanaklar idareye teslim edilir.	(5)
13	Yüklenici [PROJE VEYA SİSTEMİN ADI]'in işletim ve destek faaliyetleri esnasında 6698 sayılı Kişisel Verilerin Korunması Kanununda belirtilen "VERİ İŞLEYEN" sıfatıyla hareket eder.	(5)
14	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.	(5)

S.Nu.	Bilgi Güvenliği Gereksinimi	Açıklamalar
15	[PROJE VEYA SİSTEMİN ADI]'nde işlenen özel nitelikli kişisel verilerin güvenliği için, Kişisel Verileri Koruma Kurulunun 31 Ocak 2018 tarihli, 2018/10 sayılı Kararında belirtilen önlemler alınır.	(6), (7)
16	İşe başlama tarihini takiben [XXX gün/ay/hafta] içerisinde [PROJE VEYA SİSTEMİN ADI] kullanıcıları (Bakanlık son kullanıcıları, vatandaşlar, firmalar, kullanıcı/rol yönetimi yapan ayrıcalıklı kullanıcılar, sistem yöneticileri, yazılım geliştiriciler vb.) ve dış sistemler ile gerçekleştirilen entegrasyonlar kapsamında sisteme yapılacak her türlü erişimin kontrolü ile ilgili hususları açıklamak üzere; Bakanlık Bilgi Güvenliği Politikaları Kılavuzu ve KVKK tarafından yayımlanan "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)" dokümanında belirtildiği şekilde, "Erişim Kontrol Politikası" ve bu dokümanın parçası veya ayrı bir doküman olarak "Erişim Yetki ve Kontrol Matrisi" hazırlanır ve İdareye teslim edilir.	(5)
17	Uygulamalara oturum açmaya çalışan Bakanlık kullanıcılarının, Bakanlık İnsan Kaynakları Veri Tabanında kayıtlı ve faal bir Sağlık Bakanlığı çalışanı olup olmadığı kontrol edilir. [PROJE VEYA SİSTEMİN ADI]'nde kayıtlı olsa dâhi Bakanlık İnsan Kaynakları Veri Tabanında kayıtlı olmayan kullanıcıların sistemlere erişimi engellenir. Bu husus, Bakanlık İnsan Kaynakları Veri Tabanının bu işlem için hazır olmasını takiben İDARE tarafından talep edilmesi durumunda devreye alınır.	(8)
18	Uygulamalarda tanımlı Bakanlık kullanıcılarının, faal bir Bakanlık çalışanı olup olmadığının kontrol edilerek; Bakanlık İnsan Kaynakları Veri Tabanında faal olarak tanımlı olmayan kullanıcıların sistem yöneticisine gösterilmesini sağlayan bir arayüz oluşturulur. Bu arayüz vasıtası ile Bakanlık ile ilişiği kalıcı olarak kesilmiş personelin, uygulamalara erişim yetkilerinin iptal edilmesi sağlanır. Bu husus, Bakanlık İnsan Kaynakları Veri Tabanının bu işlem için hazır olmasını takiben İDARE tarafından talep edilmesi durumunda devreye alınır.	(8)
19	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.	(5)
20	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.	(5)

S.Nu.	Bilgi Güvenliği Gereksinimi	Açıklamalar
21	Parola değişimi yapılan tüm ekranlarda parola değişimi öncesinde, kullanıcı kimliğinin doğrulanması (eski parolanın girilmesi, SMS veya e-posta ile doğrulama vb. yöntemlerle) sağlanır.	(5)
22	Yönetici ve son kullanıcılar tarafından açılan oturumlar için zaman aşımı (time out) süreleri belirlenmelidir. Bu sürelerin parametrik olarak değiştirilmesi için gerekli yönetim arayüzleri sağlanır.	(5)
23	Tüm parolalar şifreli (özetlenmiş) olarak saklanır. Şifreleme (özetleme) işlemleri için Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunda belirtilen özetleme algoritmaları ve anahtar boyu değerleri kullanılır.	(5)
24	Sistem yönetimi maksatlı olarak sunucu/uygulamalara yapılacak erişimlerde, erişim yapan kullanıcılara sorumluluklarını açıklayan bir karşılama mesajı (onam metni) konulur.	(5)
25	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 maskıng) ve/veya şifreli olarak saklanır.	(5)
26	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.	(5)
27	Hassas bilgiler (TC Kimlik No, Kullanıcı Adı, Parola, Token vb.) hiçbir şekilde URL'ler içinde açık olarak taşınmaz.	(5)
28	Web arayüzleri ile erişilen tüm uygulamalara HTTPS protokolü kullanılarak erişilir. Bu maksatla ihtiyaç duyulan SSL sertifikaları İDARE tarafından sağlanır.	(5)
29	Sistemi oluşturan bileşenler arasında veya dış sistemler ile entegrasyon kapsamında gerçekleşen her türlü veri aktarımı/değişimi işlemleri şifrelenmiş olarak gerçekleştirilir.	(5)

S.Nu.	Bilgi Güvenliği Gereksinimi	Açıklamalar
30	Yazılımlara ait kaynak kodları İdare tarafından sağlanan Kaynak Kod Yönetim Aracında saklanır.	(5)
31	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.	(5)
32	Yazılım geliştirme esnasında, güvenli yazılım geliştirme pratikleri uygulanır. Bu amaçla İDARE tarafından hazırlanan "Güvenli Yazılım Geliştirme Kontrol Listesi" kullanılır. Güncel listeye Genel Müdürlüğün bilgi güvenliği web sitesinden erişim sağlanır.	(5)
33	Güvenli Yazılım Geliştirme Kontrol Listesinde yer alan kontrollerden PROJE'de uygulanması teknik nedenlerle mümkün olmayan maddeler, İDARE ve YÜKLENİCİ tarafından müşterek olarak belirlenir.	(5)
34	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.	(5), (9)
35	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.	(5), (9)
36	Güvenlik açıklarının çözümlendiğinin YÜKLENİCİ tarafından bildirilmesi sonrası İDARE doğrulama amaçlı olarak güvenlik testi yaptırılabilir. Tekrar edilen testlerde çıkan güvenlik açıkları, YÜKLENİCİ tarafından düzeltilir.	(5), (9)
37	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.	(5), (10)

S.Nu.	Bilgi Güvenliği Gereksinimi	Açıklamalar
38	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.	(5)
39	Alınan iz bilgileri, bütünlüğü garanti edilecek şekilde etiketlenir ve saklanır.	(5)
40	Yetkili kullanıcıların iz bilgilerine erişimi, sorgulaması ve raporlaması için ihtiyaç duyulan arayüzler sağlanır.	(5)
41	YÜKLENİCİ, canlı ortamda çalışan sistemle ilgili olarak; herhangi bir felaket, kriz ve afet durumunda, sistemin İDARE tarafından belirlenecek süre içerisinde yeniden devreye alınması için gerçekleştirilecek eylemleri ve alınacak önlemleri açıklayan iş sürekliliği planı oluşturur ve İDARE'ye teslim eder. İş sürekliliği planı, İDARE tarafından belirlenen dönemlerde test edilir, test sonuçları rapor haline getirilir ve yazılı olarak İDARE'ye teslim edilir.	(5)
42	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.	(5)

T.C.
SAĞLIK BAKANLIĞI
ARDAHAN İL SAĞLIK MÜDÜRLÜĞÜ
Teknik Şartnameler İçin Bilgi Güvenliği Gereksinimleri Listesi

Açıklamalar:

(1) Sözleşmeye konu iş kapsamında yüklenici, kuruma ait bilgilere veya bilgi işleme tesislerine fiziksel olarak veya uzaktan erişim yöntemleriyle erişim sağlayacak ise bu maddenin Teknik Şartnamelere yazılması gerekir.
(2) Sözleşmeye konu iş kapsamında alt yüklenici kullanımına müsaade edildiği durumlarda, bu madde yazılacaktır.
(3) Kurulum bilişim kaynaklarına uzaktan erişim yapılması ihtiyacı yok ise bu madde yazılmayacaktır.
(4) Sözleşmeye konu iş kapsamında kuruma özgü özel bir yazılım veya sistem geliştirilecek veya tesis edilecek ise bu madde yazılacaktır. Ancak yapılacak işin özelliği gereği, yüklenicide böyle bir uzmanlığa ihtiyaç olmadığı durumlarda bu maddenin yazılmasına gerek bulunmamaktadır.
(5) Sözleşmeye konu iş kapsamında kuruma özgü özel bir yazılım veya sistem geliştirilecek veya tesis edilecek ise bu maddeler yazılacaktır.
(6) Özel nitelikli kişisel verilerin işlendiği sistemler için geçerlidir.
(7) 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 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.
(8) Bu maddelerde yazan hususların hayata geçirilebilmesi için İKSİS/EKİM projesi tarafından gerekli servislerin sağlanması gerekmektedir. Bu maddeler yazılmadan önce, ilgili servislerin sağlanıp sağlanamayacağı konusunda İKSİS/EKİM proje ekibi ile koordine kurulması gerekmektedir.
(9) Sözleşmeye konu işin özelliğine göre, bedeli yüklenici tarafından karşılanacak şekilde, idare ve yüklenici tarafından ortak mutabakat ile belirlenecek üçüncü taraflara güvenlik testi yaptırılması hususu da dikkate alınacaktır. Güvenlik testlerinin yapılması/yaptırılması ile ilgili konular, Genel Müdürlük SOME birimi ile koordine edilecektir.
(10) Sözleşmeye konu işin özelliğine göre, bedeli yüklenici tarafından karşılanacak şekilde, idare ve yüklenici tarafından ortak mutabakat ile belirlenecek üçüncü taraflara kaynak kod analizi yaptırılması hususu da dikkate alınacaktır. Kaynak kod analizlerinin yapılması/yaptırılması ile ilgili konular, Genel Müdürlük SOME birimi ile koordine edilecektir.
(11) Yazılım ve donanım tedariki şartnamelerine konulur.

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