|  |  |  |
| --- | --- | --- |
| **S.No** | **Bilgi Güvenliği Gereksinimi** | **Açıklamalar** |
| 1 | Yüklenici sözleşmeye konu yükümlülüklerini yaparken, T.C. Sağlık Bakanlığı Burdur İl Sağlık Müdürlüğü Bilgi Güvenliği politikalarına uymak zorundadır. Bahse konu dokümanlara Müdürlüğümüz web sitesinden ([www.Burdurism.saglik.gov.tr](http://www.gaziantepism.saglik.gov.tr)) ulaşılabilir. | (1) |
| 2 | Yüklenicinin herhangi bir iş ve işleminde veya yükümlü olduğu iş ve sistemle ilgili olarak Burdur İl Sağlık Müdürlüğü 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 | Burdur İl Sağlık Müdürlüğü 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 dokümanlara, Müdürlük web sitesinden erişim sağlanır. | (1) |
| 4 | Sözleşmeye konu iş kapsamında alt yüklenici kullanılacaksa, ana yüklenici tarafından tüm alt yüklenicilere Kurumsal Gizlilik Taahhütnamesi imzalatılır ve sözleşmelerin bir sureti idareye teslim edilir. Aynı şekilde alt yüklenici çalışanları ile de Personel Gizlilik Sözleşmesi imzalanır. Alt yükleniciler ve çalışanlarına ait sözleşmeler İdareye teslim edilmeden, alt yükleniciler çalışmalara katılamaz. Alt yükleniciler ile Kurumsal Gizlilik Sözleşmesi imzalanması, asıl yüklenicinin gizlilik ile ilgili sorumluluklarını ortadan kaldırmaz veya değiştirmez. | (1), (2) |
| 5 | Kurumsal Gizlilik Taahhütnamesi ve ihaleye konu iş kapsamında çalıştırılacak anahtar personelin Personel Gizlilik Sözleşmesi imza işlemleri tamamlanmadan, yüklenici tarafından işe başlanamaz. | (1) |
| 6 | Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, Personel Gizlilik Sözleşmeleri idareye teslim edildikten sonra tanımlanır. | (1) |
| 7 | Yüklenici personelinin Müdürlük/Sağlık Tesisleri/Kurum/Birimleri bilişim kaynaklarına erişimi, İdare tarafından sağlanan Güvenli SSL VPN hizmeti üzerinden yapılır. VPN erişimi yapılabilmesi için Uzaktan Erişim Prosedürü maddeleri kapsamında Uzaktan Erişim Sözleşmesi, Kurumsal Gizlilik Taahhütnamesi ve Personel Gizlilik Sözleşmesinin idareye teslim edilmiş olması gerekir. | (3) |
| 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. | (1) |
| 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. | (4) |
| 10 | Yüklenicinin proje kapsamında kullanacağı bilgisayarlarda yer alan idareye ait veriler (yazılım kaynak kodları dâhil) Müdürlük bilgi güvenliği politikaları uyarınca şifreli olarak muhafaza edilir. | (5) |
| 11 | Projede kullanılan bilgisayarların herhangi bir nedenle kullanımdan çıkarılması durumunda, ilgili bilgisayarlar Güvenli Veri Silme Prosedürü maddeleri kapsamında güvenli silme işlemine tabi tutulur ve bununla ilgili tutanaklar idareye teslim edilir. | (5) |
| 12 | Yüklenici [**PROJE VEYA SİSTEMİN ADI**]’in işletim ve destek faaliyetleri esnasında 6698 sayılı Kişisel Verilerin Korunması Kanununda belirtilen “VERİ İŞLEYEN” sıfatıyla hareket eder. | (5) |
| 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. | (5) |
| 14 | Kullanıcıların web tabanlı uygulamalara giriş arayüzleri için adresler (link, ip vs) SSL Sertifikasına sahip olmalı ve bu arayüzler için güvenlik kodu (captcha) uygulaması yapılmalıdır. Müdürlük kullanıcıları ve vatandaşlar tarafından giriş yapılan arayüzler için farklı captcha uygulaması idare tarafından istenebilir. | (5) |
| 15 | Parola ile giriş gerektiren tüm uygulamaların, Sağlık Müdürlüğü Bilgi Güvenliği Politikaları Kılavuzunda belirtilen parola politikası ile uyumlu olması sağlanır. Doğrudan vatandaşlar tarafından giriş yapılan uygulamalar için farklı parola politikası uygulanabilir. | (5) |
| 16 | Parola değişimi yapılan tüm ekranlarda parola değişimi öncesinde, kullanıcı kimliğinin doğrulanması (eski parolanın girilmesi, SMS veya e-posta ile doğrulama vb. yöntemlerle) sağlanır. Parolaların geçerlilik süreleri ile parolaların ne asgari geçerlilik biçimleri İSM BGYS Parola Güvenliği ve Parola Yönetimi Politikalarında belirtildiği şekilde olmalıdır. | (5) |
| 17 | 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) |
| 18 | Tüm parolalar şifreli (özetlenmiş) olarak saklanır. Şifreleme (özetleme) işlemleri için Sağlık Müdürlüğü Bilgi Güvenliği Politikaları Kılavuzunda ya da teknik şartnamede belirtilen özetleme algoritmaları ve anahtar boyu değerleri kullanılır. | (5) |
| 19 | Sistem yönetimi maksatlı olarak sunucu/uygulamalara yapılacak erişimlerde, erişim yapan kullanıcılara sorumluluklarını açıklayan bir karşılama mesajı (onam metni) konulur. | (5) |
| 20 | 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. | (5) |
| 21 | Kullanıcı arayüzleri ve raporlarda bir bütün olarak görüntülenme ihtiyacı olmayan kişisel veri alanlarında Kişisel Verileri Koruma Kanunu, ilgili diğer mevzuat ve Adli Makamlarca bildirilen gizlilik kararları gereği veri maskeleme (data masking) işlemi yapılır. Hangi alanların maskeleneceği İDARE ile ortak olarak yapılacak çalışma ile belirlenir. | (5) |
| 22 | Hassas bilgiler (TC Kimlik No, Kullanıcı Adı, Parola, Token vb.) hiçbir şekilde URL’ler içinde açık olarak taşınmaz. Tamamı şifrelenmiş bir şekilde yapılır. | (5) |
| 23 | Web arayüzleri ile erişilen tüm uygulamalara HTTPS protokolü kullanılarak erişilir. Bu maksatla ihtiyaç duyulan SSL sertifikaları YÜKLENİCİ tarafından sağlanır ve kurulumu yapılır. | (5) |
| 24 | Sistemi oluşturan bileşenler arasında veya dış sistemler ile entegrasyon kapsamında gerçekleşen her türlü veri aktarımı/değişimi işlemleri şifrelenmiş olarak gerçekleştirilir. | (5) |
| 25 | Yazılımlara ait kaynak kodları İdare tarafından sağlanan Kaynak Kod Yönetim Aracında saklanır. | (5) |
| 26 | 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) |
| 27 | 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), (6) |
| 28 | Güvenlik testlerinde tespit edilen güvenlik açıklarından proje ile ilgili olanlar YÜKLENİCİ tarafından düzeltilir/ derhal idareye bildirilir. İDARE’nin ağ ve donanım altyapısı, vb. sebeplerle İDARE’den kaynaklanan güvenlik açıklarının düzeltilmesinden ve bu açıkların sistemlerde sebep olacağı gecikmelerden/kesintilerden YÜKLENİCİ sorumlu tutulamaz. | (5), (6) |
| 29 | Güvenlik açıklarının çözümlendiğinin YÜKLENİCİ tarafından bildirilmesi sonrası İDARE doğrulama amaçlı olarak güvenlik testi yaptırılabilir. Tekrar edilen testlerde çıkan güvenlik açıkları, YÜKLENİCİ tarafından düzeltilir. | (5), (6) |
| 30 | 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), (7) |
| 31 | 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) |
| 32 | Alınan iz bilgileri, bütünlüğü garanti edilecek şekilde etiketlenir ve saklanır. | (5) |
| 33 | Yetkili kullanıcıların iz bilgilerine erişimi, sorgulaması ve raporlaması için ihtiyaç duyulan arayüzler sağlanır. | (5) |
| 34 | 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) |
| 35 | 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) |

# **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. 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, Müdürlük SOME birimi ile koordine edilecektir. Uzaktan Erişim Sözleşmeleri ve diğer sözleşme/dokümanlar ıslak imzalı bir şekilde idareye teslim edilecektir. Belgelerin teslim edilmemesi durumunda uzaktan erişim hiçbir suretle açılmayacaktır.
7. 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, Müdürlük SOME birimi ile koordine edilecektir.