



**TASNİF DIŐI**  
**ADİYAMAN BELEDİYESİ**  
**TEKNİK ŞARTNAMESLER İÇİN BİLGİ GÜVENLİĞİ GEREKSİNİMLERİ**



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.Lİ.22	01.01.2021	-	-	1 / 9

**Genel Hususlar:**

1. Bu liste, BG.PO.22 Tedarikçi İlişkilerinde Bilgi Güvenliğı Politikası uyarınca Belediyemiz tarafından yapılacak tedarik işlemlerinde, ilgili dokümanlara bilgi güvenliğı 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 güvenliğı gereksinimlerinin listelenmesine gerek bulunmamaktadır.**

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

S.Nu.	Bilgi Güvenliğı Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
1	Yüklenici sözleşmeye konu yükümlülüklerini yaparken, Belediyemiz bilgi güvenliğı politikalarına uymak zorundadır. Belediyemizin bilgi güvenliğı politikaları, Bilgi Güvenliğı Politikaları Yönergesi ve Bilgi Güvenliğı Politikaları Kılavuzunda açıklanmıştır. Bahse konu dokümanlara, Belediyemiz web sitesi kurumsal bölümü veya bilgi güvenliğı web sitesinden erişim sağlanır.	√	√



**TASNİF DIŐI**  
**ADİYAMAN BELEDİYESİ**  
**TEKNİK ŞARTNAMESLER İÇİN BİLGİ GÜVENLİĐİ GEREKSİNİMLERİ**



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.Lİ.22	01.01.2021	-	-	2 / 9

S.Nu.	Bilgi GüvenliĐi Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
2	Yüklenicinin herhangi bir iş ve işleminde veya yükümlü olduĐu iş ve sistemle ilgili olarak Belediyemiz bilgi güvenliĐi 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 güvenliĐi politikalarına uyduĐu kabul edilir.	√	√
3	Adiyaman Belediyesi 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 güvenliĐi 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 deĐiştirmez.	√ (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.	√	√



**TASNİF DIŐI**  
**ADİYAMAN BELEDİYESİ**  
**TEKNİK ŞARTNAMESLER İÇİN BİLGİ GÜVENLİĞİ GEREKSİNİMLERİ**



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.Lİ.22	01.01.2021	-	-	3 / 9

S.Nu.	Bilgi Güvenliđi Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
7	Yüklenici personelinin Belediye 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)
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 içermediđi, yüklenici ve/veya üretici tarafından taahhüt edilecektir.	√	√
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.	√	√
10	Yüklenicinin (ve alt yüklenicilerin) işe başlama tarihi itibarı ile geçerli olan TÜRKAK onaylı bir belgelendirme kuruluşu tarafından verilmiş ISO/IEC 27001 Bilgi Güvenliđi Yönetim Sistemi (BGYS) Sertifikası olması gerekir.		√ (3)
11	Yüklenicinin proje kapsamında kullanacağı bilgisayarlarda yer alan idareye ait veriler (yazılım kaynak kodları dâhil), Belediye bilgi güvenliđi politikaları uyarınca şifreli olarak muhafaza edilir.		√
12	Projede kullanılan bilgisayarların herhangi bir nedenle kullanımdan çıkarılması durumunda, ilgili bilgisayarlar güvenli silme işlemine tabi tutulur ve bununla ilgili tutanaklar idareye teslim edilir.		√



**TASNİF DIŐI**  
**ADİYAMAN BELEDİYESİ**  
**TEKNİK ŞARTNAMESLER İÇİN BİLGİ GÜVENLİĐİ GEREKSİNİMLERİ**



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.Lİ.22	01.01.2021	-	-	4 / 9

S.Nu.	Bilgi GüvenliĐi Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
13	Yüklenici [PROJE VEYA SİSTEMİN ADI]'in işletim ve destek faaliyetleri esnasında 6698 sayılı Kişisel Verilerin Korunması Kanununda belirtilen "VERİ İŐLEYEN" sıfatıyla hareket eder.		√ (4)
14	Yüklenici, verilerin işlenmesi esnasında veri güvenliğinin sağlanması, erişim ve yetkilendirme gibi konularda tereddütte kalması durumunda, en seri yöntem ile İdareye başvurur ve İdarenin vereceĐi talimatlar doğrultusunda hareket eder.		√
15	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)
16	Kullanıcıların web tabanlı uygulamalara giriş ara yüzleri için güvenlik kodu (captcha) uygulaması yapılır. Belediye kullanıcıları ve vatandaşlar tarafından giriş yapılan arayüzler için farklı captcha uygulaması istenebilir.		√
17	Parola ile giriş gerektiren tüm uygulamaların, Bilgi GüvenliĐi Politikaları Kılavuzunda belirtilen parola politikası ile uyumlu olması sağlanır. Doğrudan vatandaşlar tarafından giriş yapılan uygulamalar için farklı parola politikası uygulanabilir.		√
18	Parola deĐişimi yapılan tüm ekranlarda parola deĐişimi öncesinde, kullanıcı kimliğinin doğrulanması (eski parolanın girilmesi, SMS veya e-posta ile doğrulama vb. yöntemlerle) sağlanır.		√
19	Yönetici ve son kullanıcılar tarafından açılan oturumlar için zaman aşımı (time out) süreleri belirlenebilmelidir. Bu sürelerin parametrik olarak deĐiştirilmesi için gerekli yönetim arayüzleri sağlanır.		√



TASNİF DIŐI  
**ADİYAMAN BELEDİYESİ**  
**TEKNİK ŞARTNAMESLER İÇİN BİLGİ GÜVENLİĐİ GEREKSİNİMLERİ**



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.Lİ.22	01.01.2021	-	-	5 / 9

S.Nu.	Bilgi GüvenliĐi Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
20	Sisteme oturum açıldığında, kullanıcılara en son yapılan başarılı oturum açma zamanı gösterilir ve başarısız oturum açma girişimleri hakkında bilgi verilir.		√
21	Tüm parolalar şifreli (özetlenmiş) olarak saklanır. Şifreleme (özetleme) işlemleri için Bilgi GüvenliĐi Politikaları Kılavuzunda belirtilen özetleme algoritmaları ve anahtar boyu değerleri kullanılır.		√
22	Sistem yönetimi maksatlı olarak sunucu/uygulamalara yapılacak erişimlerde, erişim yapan kullanıcılara sorumluluklarını açıklayan bir karşılama mesajı (onam metni) konulur.		√
23	Veri tabanında saklanan verilerin yetkisiz kişiler tarafından görüntülenmesini engellemek amacıyla, İDARE ile ortak olarak yapılacak çalışma sonucunda tespit edilen veri alanları, veri tabanında maskelenmiş (data masking) ve/veya şifreli olarak saklanır.		√
24	Kullanıcı arayüzleri ve raporlarda bir bütün olarak görüntülenme ihtiyacı olmayan kişisel veri alanları için veri maskeleyme (data masking) işlemi yapılır. Hangi alanların maskeleneceĐi İDARE ile ortak olarak yapılacak çalışma ile belirlenir.		√
25	Hassas bilgiler (TC Kimlik No, Kullanıcı Adı, Parola, Token vb.) hiçbir şekilde URL'ler içinde açık olarak taşınmaz.		√
26	Web arayüzleri ile erişilen tüm uygulamalara HTTPS protokolü kullanılarak erişilir. Bu maksatla ihtiyaç duyulan SSL sertifikaları İDARE tarafından sağlanır.		√



**TASNİF DIŐI**  
**ADİYAMAN BELEDİYESİ**  
**TEKNİK ŞARTNAMESLER İÇİN BİLGİ GÜVENLİĐİ GEREKSİNİMLERİ**



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.Lİ.22	01.01.2021	-	-	6 / 9

S.Nu.	Bilgi GüvenliĐi Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
27	Sistemi oluŐturan bileŐenler arasında veya dıŐ sistemler ile entegrasyon kapsamında gerçekteŐen her türlü veri aktarımı/deĐiŐimi iŐlemleri ŐifrelenmiŐ olarak gerçekteŐtirilir.		√
28	Yazılımlara ait kaynak kodları İdare tarafından saĐlanan Kaynak Kod Yönetim Aracında saklanır.		√
29	Tüm geliştirme iŐlemleri gerçekte (canlı) ortamdaki farklı bir ortamda yapılır. Bu maksatla tesis edilecek yazılım geliştirme ortamı için ihtiyaç duyulan yazılım ve donanımlar [İDARE ve/veya YÜKLENİCİ] tarafından saĐlanır. GeliŐtirilen yazılımların test edilmesi için gerçekte ortam verileri kullanılmaz.		√
30	Yazılım geliştirme esnasında, güvenli yazılım geliştirme pratikleri uygulanır. Bu amaçla İDARE tarafından hazırlanan "Güvenli Yazılım Geliştirme Kontrol Listesi" kullanılır. Güncel listeye Genel Müdürlüğün bilgi güvenliĐi web sitesinden erişim saĐlanır.		√
31	Güvenli Yazılım Geliştirme Kontrol Listesinde yer alan kontrollerden PROJE'de uygulanması teknik nedenlerle mümkün olmayan maddeler, İDARE ve YÜKLENİCİ tarafından müşterek olarak belirlenir.		√
32	İDARE gerekli gördüğünde kendi personeline ve/veya üçüncü kiŐi ve/veya firmalara güvenlik testleri yaptırabilir. Güvenlik testleri SİSTEM'in güvenlik açıklarına karşı taranmasını, analiz edilmesini, raporlanmasını ve doĐrulama testlerini kapsar.		√
33	Güvenlik testlerinde tespit edilen güvenlik açıklarından proje ile ilgili olanlar YÜKLENİCİ tarafından düzeltilir. İDARE'nin aĐ altyapısı, donanım yapılandırması vb. sebeplerle İDARE'den kaynaklanan güvenlik açıklarının düzeltilmesinden ve bu açıkların sistemlerde sebep olacağı gecikmelerden/kesintilerden YÜKLENİCİ sorumlu tutulamaz.		√



TASNİF DIŐI  
**ADİYAMAN BELEDİYESİ**  
**TEKNİK ŞARTNAMESLER İÇİN BİLGİ GÜVENLİĐİ GEREKSİNİMLERİ**



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.Lİ.22	01.01.2021	-	-	7 / 9

S.Nu.	Bilgi GüvenliĐi Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem GeliŐtirme Alımları
34	Güvenlik açıklarının çözümlendiĐinin YÜKLENİCİ tarafından bildirilmesi sonrası İDARE doğrulama amaçlı olarak güvenlik testi yaptırılabilir. Tekrar edilen testlerde çıkan güvenlik açıkları, YÜKLENİCİ tarafından düzeltilir.		√
35	İDARE, istemesi halinde kendi personeline ve/veya üçüncü kiŐi ve/veya firmaya kaynak kod analizi yaptırabilir. Analiz işlemleri esnasında talep edilmesi halinde YÜKLENİCİ tarafından analiz yapan kiŐi veya firmaya destek verilir. Kaynak kod analizleri sonucunda tespit edilen hususlara YÜKLENİCİ tarafından yapılması gereken hususlar, YÜKLENİCİ ve İDARE'nin ortak mutabakatı ile belirlenir.		√
36	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 yaptıĐı bilgileri; iç ve dış paydaŐlar için oluşturulan web servislerine iliŐkin iz bilgileri ve İDARE'nin belirleyeceĐi kritik seviyedeki diĐer işlemlere ait iz bilgileri kayıt altına alınır.		√
37	Alınan iz bilgileri, bütünlüĐü garanti edilecek şekilde etiketlenir ve saklanır.		√
38	Yetkili kullanıcıların iz bilgilerine erişimi, sorgulaması ve raporlaması için ihtiyaç duyulan ara yüzler sağlanır.		√



**TASNİF DIŐI**  
**ADİYAMAN BELEDİYESİ**  
**TEKNİK ŞARTNAMESLER İÇİN BİLGİ GÜVENLİĞİ GEREKSİNİMLERİ**



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.Lİ.22	01.01.2021	-	-	8 / 9

S.Nu.	Bilgi Güvenliđi Gereksinimi	Genel Mal ve Hizmet Alımları	Yazılım/Sistem Geliştirme Alımları
39	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.		√
40	06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 2019/12 sayılı Bilgi ve İletişim Güvenliđi Tedbirleri konulu Cumhurbaşkanlığı Genelgesi'nin 12. Maddesi uyarınca; sözleşme kapsamında 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 yükleniciden <b>BG.SZ.05 Arka Kapı Taahhünamesi</b> alınır.	√(7)	√

**Açıklamalar:**

- (1) Sözleşmeye konu iş kapsamında alt yüklenici kullanımına müsaade edildiđi 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 bozmayacağıнын değerlendirildiđi durumlarda, bu maddenin yazılması tavsiye edilmektedir.
- (4) İhaleye konu iş kapsamında kişisel verilerin işlenmesi söz konusu olduğü durumlarda yazılacaktır.
- (5) Özel nitelikli kişisel verilerin işlendiđi 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





TASNİF DIŐI  
**ADİYAMAN BELEDİYESİ**  
**TEKNİK ŐARTNAMELER İÇİN BİLGİ GÜVENLİĐİ GEREKSİNİMLERİ**



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.Lİ.22	01.01.2021	-	-	9 / 9

yazılım geliştirme araçları/platformlar ve VTYS yazılımları bu isteĐi gerçekleŐtirmek için gereken fonksiyonları desteklemeyebilir. Bu gibi sebeplerle, bu maddenin gereklerinin yapılabilmesi için ciddi yatırımlar yapılmasına ihtiyaç duyulabilir. Bu maddenin Őartnameye yazılması halinde olası etkilerinin Proje Yönetimi ekipleri/ihitiyaç 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 deĐerlendirilmektedir.

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