1. Amaç

Bu dokümanın amacı, BGYS kapsam dokümanında belirtilen şube müdürlüklerinde uygulanacak olan bilişim ürün ve hizmet alımlarında teknik şartnamelerde yer alması gereken asgari BGYS gereksinimlerinin karşılanması amacı ile hazırlanmıştır.

2. Kapsam

Bu belge, kapsam dokümanında belirtilen şube müdürlüklerinde gerçekleştirilecek bilişim ürün ve hizmet alımlarında teknik şartnamelerde yer alması gereken asgari BGYS gereksinimlerini kapsar.

3. Tanımlamalar ve Kısaltmalar

Kurum: Meteoroloji Genel Müdürlüğü,
BGYS: Bilgi Güvenliği Yönetim Sistemi,
Personel: Kuruma bağlı çalışan kimseler,

4. Uygulama

İhaleye konu mal ve/veya hizmet alımı kapsamında; 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 veya kuruma ait gizli kalması gereken bilgilerin bir kısmı veya tamamı teslim edilecek" ise aşağıdaki listedeki uygun maddeler teknik şartnamelere ve/veya idari şartnamelerin ilgili bölümlerine yazılacaktır.

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

SN	Bilgi Güvenliği Gereksinimi	Mal ve/veya Hizmet Alımı	Yazılım, Güncelleme, Danışmanlık, Eğitim vb.
1	Yüklenici sözleşmede yer alan yükümlülüklerini yerine getirirken, Kurumun BGYS politikalarına uymak zorundadır. Kurumun BGYS politikalarına **https://www.mgm.gov.tr/bgys** adresinden erişim sağlanır.	+	+
2	Yüklenici, Kurumun BGYS politikalarına aykırı hareket ettiğinin tespit edilmesi halinde, İdare tarafından sözlü ve/veya yazılı olarak sorumlulukların yerine getirilmesine ilişkin uyarılır.	+	+
3	Kurumun BGYS politikaları uyarınca, idareye ait bilgilerin korunması maksadıyla, yükleniciler ile **BGYS-SZ-01: Üçüncü Taraf Gizlilik Sözleşmesi**, iş kapsamında çalışacak olan yüklenici personeli ile **BGYS-SZ-02: Üçüncü Taraf Çalışanları Gizlilik Sözleşmesi** imzalanır. Sözleşme belgelerine https://www.mgm.gov.tr/bgys adresinden ulaşılabilir.	+	+

SN	Bilgi Güvenliği Gereksinimi	Mal ve/veya Hizmet Alımı	Yazılım, Güncelleme, Danışmanlık, Eğitim vb.
4	Sözleşmeye konu iş kapsamında alt yüklenici kullanılacaksa, ana yüklenici tarafından tüm alt yüklenicilere **BGYS-SZ-01: Üçüncü Taraf Gizlilik Sözleşmesi,** alt yüklenici çalışanları ile de **BGYS-SZ-02: Üçüncü Taraf Çalışanları Gizlilik Sözleşmesi** imzalatılır ve belgelerin ıslak imzalı suretleri idareye teslim edilir. Alt yükleniciler ve çalışanlarına ait sözleşmeler İdareye teslim edilmeden, alt yükleniciler çalışmalara katılamaz. Alt yükleniciler ile BGYS-SZ-02: Üçüncü Taraf Çalışanları Gizlilik Sözleşmesi imzalanması, asıl yüklenicinin gizlilik ile ilgili sorumluluklarını ortadan kaldırmaz veya değiştirmez.	+ (1)	+ (1)
5	**BGYS-SZ-01: Üçüncü Taraf Gizlilik Sözleşmesi** ve ihaleye konu iş kapsamında çalıştırılacak personellerin **BGYS-SZ-02: Üçüncü Taraf Çalışanları Gizlilik Sözleşmesinin** imza işlemleri tamamlanmadan, yüklenici/alt yüklenici tarafından işe başlanamaz.	+	+
6	Yüklenici/alt yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, **BGYS-SZ-02: Üçüncü Taraf Çalışanları Gizlilik Sözleşmesi** idareye teslim edildikten sonra tanımlanır.	+	+
7	Yüklenici/alt yüklenici personelinin uzaktan Kurum bilişim kaynaklarına erişimi, İdare tarafından sağlanan VPN hizmeti üzerinden yapılır. VPN erişimi yapılabilmesi için **BGYS-FR-12: Üçüncü Taraf VPN Erişim Talep Formu** idareye teslim edilmiş olması gerekir.	+ (2)	+ (2)
8	Yüklenici, çalıştırılacağı personelin son **30 gün** içerisinde alınmış adli sicil belgesini idareye bildirir. (Çalışanların TCK'nın 53'ncü maddesinde belirtilen süreler geçmiş olsa bile devletin güvenliğine karşı işlenen 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 BGYS Sertifikası** olması gerekir.		+ (3)
10	Yüklenicinin proje kapsamında kullanacağı bilgisayarlarda yer alan idareye ait veriler (yazılım kaynak kodları dâhil), Kurumun BGYS politikalarına uygun şekilde muhafaza edilir.		+
11	Yüklenici işin konusu işletim ve destek faaliyetleri esnasında 6698 sayılı Kişisel Verilerin Korunması Kanununda belirtilen "Veri İşleyen" sıfatıyla hareket eder.		+ (4)
12	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)
13	Kuruma özel web tabanlı yazılım projesi ise Kullanıcıların web tabanlı uygulamalara giriş arayüzleri için güvenlik kodu (captcha), sms, e-posta, mobil imza üzerinden en az biri ile doğrulama yapılmalıdır.		+
14	Parola ile giriş gerektiren tüm uygulamalar **BGYS-PR-09: Erişim Kontrol Prosedürü'nde** yer alan parola politikası ile uyumlu olması sağlanır.		+
15	Parola değişimi yapılan tüm ekranlarda parola değişimi öncesinde, kullanıcı kimliğinin doğrulanması (eski parolanın girilmesi, SMS veya e-posta ile doğrulama vb. yöntemlerle) sağlanır.		+
16	Yönetici ve son kullanıcılar tarafından açılan oturumlar için zaman aşımı (time out) süreleri olmalıdır.		+
17	Tüm parolalar şifreli (özetlenmiş) olarak saklanır. Şifreleme (özetleme) işlemleri için **BGYS-PR-10: Kriptografik Kontrollerin Kullanımı Prosedürü'**nde belirtilen özetleme algoritmaları ve anahtar boyu değerleri kullanılır.		+

SN	Bilgi Güvenliği Gereksinimi	Mal ve/veya Hizmet Alımı	Yazılım, Güncelleme, Danışmanlık, Eğitim vb.
18	Hassas bilgiler (T.C. Kimlik No, Kullanıcı Adı, Parola, Token vb.) hiçbir şekilde url'ler içinde açık olarak taşınmaz.		+
19	Web arayüzleri ile erişilen tüm uygulamalara SSL sertifikaları idare tarafından sağlanacak şekilde HTTPS protokolü kullanılarak erişilir.		+
20	Sistemi oluşturan bileşenler arasında veya dış sistemler ile entegrasyon kapsamında gerçekleşen her türlü veri aktarımı/değişimi işlemleri şifrelenmiş olarak gerçekleştirilir.		+
21	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 Yüklenici] tarafından sağlanır. Geliştirilen yazılımların test edilmesi için gerçek ortam verileri kullanılmaz.		+
22	Yazılım geliştirme esnasında, güvenli yazılım geliştirme pratikleri uygulanır. Bu amaçla İdare tarafından hazırlanan BGYS-FR-23: Güvenli Yazılım Geliştirme Süreci Kontrol Formu, BGYS-PR-14 Bilgi Sistemlerinin Güvenlik Gereksinimleri Prosedürü ile Tübitak Bilgem Güvenli Yazılım Geliştirme Kılavuzu **referans olarak** kullanılmalıdır.		+
23	Güvenli Yazılım Geliştirme Kontrol Listesinde yer alan kontrollerden PROJE'de uygulanması teknik nedenlerle mümkün olmayan maddeler, İdare ve Yüklenici tarafından müşterek olarak belirlenir.		+
24	İdare kendi personeline ve/veya üçüncü kişi ve/veya firmalara güvenlik testleri yaptırabilir. Güvenlik testleri CVE (Common Vulnerabilities and Exposures) güvenlik seviyesi yüksek ve daha üstü güvenlik açıklarına karşı taranmasını, analiz edilmesini, raporlanmasını ve doğrulama testlerini kapsar.	+ (8)	+
25	Güvenlik testlerinde tespit edilen ve/veya bilinen güvenlik açıkları Yüklenici tarafından düzeltilir. Yüklenici'nin ağ altyapısı, donanım yapılandırması vb. sebeplerle oluşturacağı güvenlik açıklarının düzeltilmesi sırasında yaşanabilecek veri ifşası, veri kaybı, gecikme, kesinti vb. durumlarda Yüklenici'nin sorumluluğu açık şekilde belirtilecektir.	+ (8)	+
26	Güvenlik açıklarının çözümlendiğinin Yüklenici tarafından bildirilmesi sonrası İdare doğrulama amaçlı olarak güvenlik testi yaptırılabilir. Tekrar edilen testlerde çıkan güvenlik açıkları, Yüklenici tarafından düzeltilir.	+ (8)	+
28	İdare, istemesi halinde kendi personeline ve/veya üçüncü kişi ve/veya firmaya kaynak kod analizi yaptırabilir. Analiz işlemleri esnasında talep edilmesi halinde Yüklenici tarafından analiz yapan kişi veya firmaya destek verilir. Kaynak kod analizleri sonucunda tespit edilen hususlara Yüklenici tarafından yapılması gereken hususlar, Yüklenici ve İdare'nin ortak mutabakatı ile belirlenir.		+ (9)
29	Yüklenici firma Sözleşme aşamasında Kep adresini idareye bildirmeli ve garanti süresince tüm yazışmalar kep adresi üzerinden yapılmalıdır.	+	+
30	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.		+

SN	Bilgi Güvenliği Gereksinimi	Mal ve/veya Hizmet Alımı	Yazılım, Güncelleme, Danışmanlık, Eğitim vb.
31	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 **BGYS-TH-04: 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)
32	İhaleye konu iş kapsamında yüklenici tarafından işletme, bakım ve idame desteği sağlanacak ise ilgili teknik şartnamelere arıza türleri, arızalara ilk müdahale ve sorun giderme süreleri (SLA: Service Level Agreement) ile bu sürelere uyulmaması halinde uygulanacak cezai yaptırımlar açık şekilde belirtilmelidir. Ayrıca arızanın giderilmesi için parça temini, yazılım yükseltme vb. gerekiyorsa kimin tarafından temin ve finanse edileceği açık şekilde belirtilmiş olmalıdır. **Örnek:** Yüksek: Sistemin çalışmaması, açılmaması, cevap vermemesi, beklenen görevi yapamaması veya durmasına yol açabilecek arıza. Orta: Sistemin tam kapasite çalışamaması, aşırı yük, yavaşlık veya bazı fonksiyonlarının doğru çalışmaması ya da kullanıcıların tüm fonksiyonları kullanmasına engel olabilecek arızalar. Düşük: Sistemde yaşanan performans sorunları, minör güncelleme ihtiyaçları, kısmi teknik destek ihtiyaçları vb. türündeki arızalar Yüklenici, aşağıda temel şartları belirtilen SLA sürelerine göre müdahale ve çözüm gerçekleştirecektir. **Seviye** / **İlk Müdahale (Saat)** / **Arıza Giderme (Saat)** Yüksek / 8 / 24 Orta / 16 / 48 Düşük / 24 / 72	+	+

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) Yapılacak işin konusu kapsam dışı değilse veya 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.

(8) Donanım temini yapılacaksa ilgili donanımların firmware, bios, servis yazılımı vb. üzerinde yayınlanmış açıklar var ise gerekli güncelleme yaptırılmalıdır.

(9) Kuruma özel geliştirilmiş ve kaynak kodu kurumda olan yazılım veya kurumun bağlı olduğu üst Kurumlar tarafından özel olarak doğrulama isteniyorsa.

5. İlgili Dokümanlar

1. BGYS-KP-01 Kapsam Dokümanı
2. BGYS-SZ-01 Üçüncü Taraf Gizlilik Sözleşmesi
3. BGYS-SZ-02 Üçüncü Taraf Çalışanları Gizlilik Sözleşmesi
4. TR EN ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı