T.C.

ULAŞTIRMA VE ALTYAPI BAKANLIĞI

TÜRASAŞ GENEL MÜDÜRLÜĞÜ

ISO 27001 BGYS Danışmanlık İşlerinin İşletilmesine Yönelik Destek Hizmeti Alımına İlişkin Teknik Şartname

2024, Ankara

1. İçindekiler

1. Genel Tanımlar

İDARE : Bu şartnamede, işin sahibi sıfatı ile Ulaştırma ve Altyapı Bakanlığı TÜRASAŞ Genel Müdürlüğü
FİRMA : Taahhüt işini yüklenecek firma
YÜKLENİCİ : Taahhüt işini yüklenen firma
İSTEKLİ : Teklif veren firma
PROJE : İşbu ihale çerçevesinde gerçekleştirilecek tüm faaliyetler
BGYS : Bilgi Güvenliği Yönetim Sistemi

1.1. Teknik Şartnamede kullanılan teknik kısaltmaların açıklamaları aşağıdadır.
CISSP : Certified Information Systems Security Professional,
ISSAP: Information Systems Security Architecture Professional,

2. İşin Konusu ve Kapsamı

2.1. T.C. Ulaştırma Ve Altyapı Bakanlığı TÜRASAŞ Genel Müdürlüğü bünyesinde yürütülen hizmetlerin ve bu hizmetlerde kullanılan bilgilerinin gizliliğini, bütünlüğünü ve sürekliliğini sağlamak amacıyla ulusal ve uluslararası kabul görmüş standartlar, mevzuatlar doğrultusunda ISO 27001 BGYS:2013 Standardı süreçlerine yönelik yapılacak danışmanlık çalışmalarını kapsamaktadır.

3. Genel Şartlar

3.1. Bu şartnamede tanımlanan hizmetleri içeren projenin toplam süresi 90 (doksan) gündür.
3.2. YÜKLENİCİ'nin Ankara'da yerleşik ofisi bulunacaktır.
3.3. YÜKLENİCİ'nin Millî Savunma Bakanlığı tarafından verilen Tesis Güvenlik Belgesi bulunacaktır.
3.4. YÜKLENİCİ, bu şartnamede tarif edilen hizmetlerin ulusal ve uluslararası standartlar ile sektör en iyi uygulamalarına uygun olarak icra edilmesini sağlamak üzere gerekli çalışmalara metodolojik bakış açısı ve uluslararası siber güvenlik yaklaşımıyla yön verebilmek için projede çalışacak ekipler haricinde gerektiğinde bu ekipleri destekleyici olmak en az aşağıdaki sertifikasyonlara sahip personel bulunduracaktır.
3.5. En az 1(bir) adet ISC2 CISSP (Certified Information Systems Security Professional),
3.6. En az 1 (bir) adet PMP (Project Management Professional),
3.7. En az 3 (üç) adet ISO 27001:2022 Lead Auditor,
3.8. YÜKLENİCİ'nin; Kalite Yönetim Sistemi ISO 9001:2015, TSE Hizmet Yeterlilik Belgesi, Müşteri Memnuniyeti Yönetim Sistemi ISO 10002:2018, Bilgi Güvenliği Yönetim Sistemi ISO 27001:2017, Bilgi Teknolojileri Hizmet Yönetim Sistemi ISO/IEC 20000-1:2018, İş Sürekliliği Yönetim Sistemi ISO 22301:2019, İş Sağlığı ve Güvenliği Yönetim Sistemi ISO 45001:2018, Kişisel Veri Yönetim Sistemi ISO 27701 belgesi ve Dijital Dönüşüm Ofisi tarafından verilen "Bilgi ve İletişim Güvenliği Uyum Denetimi Hizmeti Sağlayan Firma Belgesi", bulunacaktır.
3.9. YÜKLENİCİ bünyesinde Bilgi ve İletişim Güvenliği Rehberi uyum denetimlerini gerçekleştirebilecek gerekli şartları sağlayan en az 2 (iki) D1 ve/veya D2 belgeli denetçi ile en az 1 (bir) D1 ve/veya D2 tipi belgeli baş denetçi tam zamanlı olarak çalışıyor olmalıdır.
3.10. YÜKLENİCİ ve İDARE hizmet başlangıcında bu hizmete özel bir gizlilik sözleşmesi imzalayacaktır.
3.11. YÜKLENİCİ, sözleşmenin imzalanmasından itibaren en geç 10 (on) iş günü içerisinde, şartname kapsamında verilecek hizmetler ile ilgili detaylı proje planı hazırlayarak İDARE'ye sunacaktır.

3.12. YÜKLENİCİ, bu şartname kapsamında verilecek tüm hizmetleri koordine etmek ve projenin planlandığı gibi ilerlemesini kontrol etmek üzere bir proje yöneticisi görevlendirecektir.

3.13. YÜKLENİCİ personelinden proje kapsamında çalışacak olanların YÜKLENİCİ ile imzaladıkları gizlilik sözleşmeleri İDARE'ye sunulacaktır. İDARE ile de ayrıca Güvenlik Taahhütnamesi imzalanacaktır.

3.14. YÜKLENİCİ, proje başlangıcında sunacağı iş planı, projenin planlama aşamasında İDARE ile birlikte detaylandıracak ve İDARE onayına sunacaktır.

3.15. YÜKLENİCİ personeli, sistem üzerinde yapacağı her türlü iş, işlem ve müdahaleyi İDARE personeli eşliğinde/izniyle yapacaktır.

3.16. YÜKLENİCİ, çalıştıracağı her personelin, İDARE yetkililerinin kontak noktası personelin kimler olduğunu, mesai içi ve mesai dışı saatlerde bu kişilere ulaşılabilecek telefon numaraları konusunda bilgilenmesini sağlamaktan sorumlu olacaktır.

3.17. Proje kapsamında hazırlayacağı ve İDARE'ye sunacağı bütün dokümanları Türkçe olarak hazırlayacaktır. Teknik detaylar için İngilizce terimler kullanıldığı durumlarda parantez içinde Türkçe 'si yazılacaktır

4. ISO 27001 Bilgi Güvenliği Yönetim Sistemi İşletim Danışmanlığı

4.1. BGYS İşletim Danışmanlığı

4.1.1. Bilginin öneminin giderek arttığı günümüzde de bu altyapının güvenliğinin sağlanması için uluslararası düzeyde kabul görmüş olan TS ISO/IEC 27001 BGYS'nin iyileştirilmesi barındırılan bilgilerin güvenliğinin sağlanmasında sistematik bir sürecin izlenmesinde İDARE'ye katkı sağlayacaktır. Bu kapsamda, tedarik edilecek BGYS Danışmanlığı Hizmeti aşağıdaki ana başlıklardan oluşacaktır.

- BGYS'nin İyileştirilmesi
- İç Tetkik
- Yönetimin Gözden Geçirmesi
- BGYS Sertifikasının Devamlılığının Sağlanması
- Eğitimler

4.1.2. Bilgi Güvenliği Yönetim Sistemi İşletim Danışmanlığı kapsamında gerçekleştirilecek çalışmalar TÜRASAŞ Ankara Genel Müdürlüğü, TÜRASAŞ Sivas Bölge Müdürlüğü, TÜRASAŞ Eskişehir Bölge Müdürlüğü ve TÜRASAŞ Sakarya Bölge Müdürlüğü kapsamında gerçekleştirilecektir. Bölge Müdürlükleri ile online (uzaktan) çalışmalar gerçekleştirilerek, iç denetim ve dış denetime eşlik çalışmaları yerinde gerçekleştirilecektir.

4.2. BGYS'nin İyileştirilmesi

4.2.1. Bu çalışma ile Kurum içerisinde işletilmekte olan TS ISO/IEC 27001 Standardına uygun BGYS'nin işletimi ve ihtiyaç duyulan iyileştirmelerin yapılması için danışmanlık sağlanacaktır. Bu kapsamda Yüklenici'nin yapması beklenen işler aşağıda belirtilmiştir.

4.2.2. Kurumda bir boşluk analizi yapılarak bilgi güvenliği ile ilgili işlettiği süreçler ve aldığı önlemler ISO 27001 standardının isterlerine göre değerlendirilecek ve İDARE'ye raporlamasını yapacaktır.

4.2.3. Boşluk analizi sonuçlarına göre İdare yapısına uygun ve en az ISO 27003 Bilgi teknolojisi- Güvenlik teknikleri- Bilgi güvenliği yönetim sistemi uygulama kılavuzunda belirtilen hususları karşılayacak şekilde BGYS ekibi organizasyonun mevcudiyeti kontrol edilerek, gerekiyorsa güncellemelerin yapılması için çalışmalar yapılacaktır.

4.2.4. Boşluk analizi sonuçlarını, proje planını, organizasyon yapısını ve üst yönetici bilgi güvenliği farkındalık konularını içeren, üst yönetimin proje desteğinin alınmasını sağlamak amacıyla üst yönetim sunumu yapılacaktır.

4.2.5. YÜKLENİCİ, Standardın Madde 4-10 arasında belirtilen BGYS kapsamında hazırlanmış olan zorunlu dokümanları gözden geçirecek, risk değerlendirme sonuçlarına ve BGYS kapsamındaki değişikliklere göre güncellenmesi gereken dokümanları belirleyecek ve güncellenmesini sağlayacaktır.

4.2.6. Güncellenen temel dokümanlar İdare'nin onayına sunulacaktır.

4.2.7. BGYS ekibine yeni katılan personel var ise 1 gün sürecek şekilde, ISO 27001:2013 standardının uygulanması, denetlenmesi, sürdürülmesi ve proje adımlarını anlatan bir eğitim verilecektir.

4.2.8. ISO 27001:2013 kapsamında bulunan varlık envanteri Bilgi Sistemleri Birimi ile birlikte gözden geçirilerek, güncellenmesi için danışmanlık verilecektir.

4.2.9. Güncellenen varlık envanterine göre daha önceki risk değerlendirme çalışmaları da dikkate alınarak, İDARE'yi etkileyebilecek güvenlik riskleri tespit edilerek Risk Değerlendirme Listesi güncellenecektir.

4.2.10. YÜKLENİCİ, İDARE'nin varlıklarına yönelik yeni risklerin değerlerinin hesaplayacak ve önceliklendirilerek mevcut risk çıktılarına eklemesini gerçekleştirecektir.

4.2.11. YÜKLENİCİ, risk işleme aktivitelerini planlayacaktır.

4.2.12. YÜKLENİCİ, mevcut risk işleme planında yer alan faaliyetlerin takibini ve güncellemesini gerçekleştirecektir.

4.2.13. YÜKLENİCİ, Mevcut Uygulanabilirlik Bildirgesini gözden geçirecek, yeni oluşturulan dokümanlar olursa bu dokümanların referans olarak eklenmesini sağlayarak Uygulanabilirlik Bildirgesini güncelleyecektir.

4.2.14. İdarenin risk işleme kararlarına göre uygulanabilirlik bildirgesi göz önünde bulundurularak BGYS için zorunlu dokümanların mevcudiyeti kontrol edilecek, mevcut dokümanlar gözden geçirilecek, gerekiyorsa güncellenmesi yapılacaktır, EK-A Kontrol Maddelerine karşılık gelen dokümantasyona göre ihtiyaç olan dokümanların oluşturulması sağlanacaktır.

4.2.15. Oluşturulacak dokümanlar İdare tarafından kontrol edilecek ve değişiklik talepleri Yüklenici' ye bildirilecektir. Yüklenici her bir doküman için bildirim tarihinden sonra en geç 5 (beş) iş günü içerisinde revize dokümanı İdare ile paylaşacaktır.

4.2.16. Dokümanların son hali İdare tarafından onaylanacaktır.

4.2.17. Dokümanların ilgili kullanıcılara duyurulması ve yaygınlaştırılması İdare'nin sorumluluğundadır.

4.2.18. Çalışmalar hibrit gerçekleştirilecektir.

4.3. İç Tetkik

4.3.1. Risk işleme faaliyetleri tamamlandıktan sonra YÜKLENİCİ tarafından İDARE personelinin de katılımı ile iç tetkik gerçekleştirilecektir.

4.3.2. İç tetkikler aşağıdaki hususlar göz önüne alınarak yapılacaktır:

4.3.3. İç tetkik planı prosedürde belirtildiği şekilde oluşturulacak ve idare ile paylaşılacaktır.

4.3.4. İç tetkik, proje içerisinde yer almamış ve ISO 27001 Baş Denetçi sertifikasına sahip denetçi tarafından gerçekleştirilecektir.

4.3.5. İç tetkikte tespit edilen bulguların giderilmesi için İdare'ye yol göstericilik yapılacaktır.

4.3.6. İç tetkik sonrası düzeltici faaliyet kayıtları İDARE ile birlikte oluşturulacaktır.

4.4. Yönetimin Gözden Geçirmesi

4.4.1. Yüklenici, İdare ile birlikte yapılan tüm çalışmaları ve standardın 9.3 maddesi gereği konuları içeren bir rapor ve YGG sunumunu hazırlayacaktır.

4.4.2. Yüklenici, İdarenin istemesi durumunda YGG toplantısına katılacaktır.

4.5. BGYS Sertifikası'nın Devamlılığının Sağlanması

4.5.1. Proje kapsamında iyileştirilen ISO 27001:2013 versiyonuna göre kurulmuş olan işletilen BGYS'nin, TÜRKAK akreditasyonu olan bağımsız bir denetçi kuruluş tarafından denetlenecektir.

4.5.2. Yüklenici belgelendirme sürecinde İdare ye destek olmak için projede görev almış en az bir danışmanını belgelendirme denetimi sürecinde eşlik etmesi için idare yerleşkesinde bulunduracaktır.

4.5.3. Yüklenici, yer tesliminden sonra en geç 90 (doksan) gün içerisinde İdare'nin ve Yüklenici'nin belirleyeceği bağımsız bir denetçi kuruluşa başvuruda bulunulacak ve denetime girilecek şekilde çalışmalarını tamamlayacaktır.

4.5.4. Yüklenici, denetimler esnasında tespit edilecek bulguların giderilmesi için aksiyon önerilerini için İdare'ye sunacaktır. Dokümantasyon süreçlerine ilişkin bulguların düzeltilmesi için doküman güncelleme çalışmalarını Yüklenici gerçekleştirecek, süreçlerin işletilmesine ilişkin bulguların düzeltilmesi için Düzeltici Faaliyet önerilerini İdare'ye sunacaktır.

4.5.5. Danışmanlık hizmeti, Bilgi Güvenliği Yönetim Sisteminin TS ISO/IEC 27001:2013 standardına uygunluk belgesinin devamlılığının sağlanması ile tamamlanacaktır.

4.6. BGYS Eğitimleri

4.6.1. Eğitimlerin dili Türkçe olacaktır.

4.6.2. Eğitimler ile ilgili notlar İdare ile eğitimlerden önce paylaşılacaktır.

4.6.3. BGYS Temel Eğitimini verecek proje ekibi içerisinde yönetim sistemi danışmanlığı konusunda yeterliliğini göstermek için TS ISO/IEC 27001 Baş Denetçi sertifikasına sahip olacaktır.

4.6.4. YÜKLENİCİ, proje süresince kurum personelleri için online BGYS farkındalık eğitimi verecektir.

4.7. Proje 90 iş günü içerisinde tamamlanacaktır.

Selim ÇEVİK
Tekniker

Bilgi Sistemleri Daire Başkanı