İSTANBUL TİCARET ÜNİVERSİTESİ

BİLGİ VE İLETİŞİM GÜVENLİĞİ DANIŞMANLIĞI İŞİ

TEKNİK ŞARTNAMESİ

1. KONU VE TANIMLAR

1.1. KONU

Bilgilerin dijital ortamlara taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması nedeniyle oluşan güvenlik risklerinin azaltılması veya etkisiz kılınması; özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla alınacak tedbirleri açıklamak maksadıyla 06.07.2019 tarihli ve 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır.

Mezkûr Genelge kapsamında Üniversitemiz birimleri tarafından Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin (CBDDO) Bilgi ve İletişim Güvenliği Rehberi çerçevesinde rehber uyum çalışmaları gerçekleştirilecektir.

1.2. KAPSAM

Bu Teknik Şartname, Bilgi ve İletişim Güvenliği Rehberi'nde "Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci" olarak ifade edilen ve aşağıdaki maddelerde detaylandırılan iş ve işlemler bağlamında eğitim ve süreç yönetim danışmanlığı hizmeti alımını kapsamaktadır.

1.3. TANIMLAR

İşbu Teknik Şartname içinde kullanılan aşağıdaki kelime ve deyimler, içinde geçtiği metin farklı bir anlam vermedikçe aşağıda tarif edildiği gibi anlaşılacaktır.

REHBER: Bilgi ve İletişim Güvenliği Rehberi (https://www.cbddo.gov.tr/bgrehber)

KURUM: İstanbul Ticaret Üniversitesi

İDARE: Genel Sekreterlik

YÜKLENİCİ: Kurum ile sözleşme imzalayan istekli firma

2. GENEL ŞARTLAR

2.1. İstekliler, şartnamede belirtilen iş ve işlemleri maliyetlendirebilmek amacıyla İdare'nin nezaretinde yerinde keşif yapabilir.

2.2. Yüklenici, sözleşme imzalandığı gün itibari ile 10 (on) takvim gün içerisinde bir eylem planı oluşturarak İdare'ye sunacak ve İdare'nin onayı sonrasında faaliyetlerini bu takvim/plana göre yürütecektir. Eylem planı; kilometre taşlarını, iş adımlarını, zamanlama planını, toplantıları içerecektir.

2.3. Yüklenici personeli sistem üzerinde yapacağı her türlü iş, işlem ve müdahaleyi İdare personeli gözetim ve denetiminde gerçekleştirecektir. Yüklenici uzman personeli sistemlere ya da sistemlerin bulunduğu mekânlara fiziksel olarak müdahale edebilmek için İdare'nin onayını almak zorundadır.

2.4. Yüklenici, bu proje kapsamında hizmetlerini yerine getirmek için gerekli tüm kullanıcı cihazlarını ve/veya yazılımlarını beraberinde getirecek, İdare'den bu konuda herhangi bir talepte bulunmayacaktır.

2.5. Yüklenici, Kurum'un sürece dâhil olan tüm birimlerinde yapılması muhtemel çalışmaları analiz ve gereksinim raporları ile belirleyecektir.

2.6. Yüklenici, İdare tarafında bu Teknik Şartname'de belirtilen iş ve işlemleri gerçekleştirecek komisyonun oluşturulması için de hizmet verecektir. Bu hizmet, ilgili birim temsilcilerinin ve üst yönetimin katılımıyla sorumluluk ve yetkilerin ne olması gerektiğinin görüşülmesi, bilgi ve iletişim güvenliği ile ilgili işleri yönetecek komisyonun ve ekibin belirlenmesi ve bunların rol ve sorumluluklarının tanımlanması adımlarından oluşacaktır.

2.7. Yüklenici, Rehber uyum çalışmaları için Sözleşme tarihinden itibaren 15 (on beş) takvim günü içerisinde en az aşağıda belirtilen çerçevede kendi proje ekibini oluşturacaktır.

- Proje Yöneticisi (Bilgi Güvenliği Danışmanı)
- Proje Yönetici Asistanı (Proje Yöneticisi & Raportör)
- Siber Güvenlik Uzmanı (OSWP, Assessing and Exploiting Control Systems & IIoT, Certified Red Teaming Expert, Wi-Fi Security Expert)

2.8. İhale konusu işte İdare'nin onayı ile altyüklenici çalıştırabilir. Altyüklenici çalıştırılması halinde altyükleniciye yaptırılması düşünülen işlerin listesi "Yeterlilik Bilgiler Tablosunda" sunulacaktır.

2.9. Bilgi ve iletişim güvenliği denetimi öncesinde yapılması gereken tüm çalışmalar 1 Aralık 2022 tarihinden önce bitirilmelidir. Aktif danışmanlık süresi 12 ay boyunca devam edecektir. Tarafların uzlaşması durumunda ek protokol ile danışmanlık süreci yenilenecektir.

2.10. Yüklenici, hizmet süresi boyunca şahit olabileceği ve Kurum için hassasiyet arz eden tüm bilgileri koruyacaktır. Bu bilgileri Kurum'un yazılı onayı olmadan kamuya açık herhangi bir ortamda açıklamayacaktır.

2.11. Yüklenici, hizmet süresi boyunca hazırladığı tüm dijital ve fiziki dokümanları iş bitiminde Kurum'a teslim edecek ve kendi arşiv veya cihazları (bilgisayar vb.) üzerinde bulunan tüm kopyalarını güvenli şekilde imha edecektir.

2.12. Yüklenici Teknik Şartname'yi açık, anlaşılır ve yoruma gerek bırakmayacak şekilde cevaplayacak ve okuyup kabul ettiğini belirtecektir.

2.13. Yüklenici, şartnameye bütün olarak teklif verecek olup parçalı teklifler kabul edilmeyecektir.

3. YAPILACAK İŞLER

3.1. Bilgi ve iletişim güvenliğine ilişkin varlık grupları belirlenecektir.

Bu varlık gruplarının niteliği temel olarak şöyledir: Elektronik ve/veya fiziksel ortamlarda yer alan, iletişim yoluyla aktarılabilen bilgiyi içeren ve kurumun iş süreçleri açısından değer taşıyan,

- Tüm bilgi ve bilgi işleme olanakları,
- Bilgiyi kullanan ve taşıyan personel,
- Bilgiyi barındıran fiziksel mekânlar.

Rehber çerçevesinde Kurum'un mülkiyetinde bulunan varlıklar, varlık grupları ve alt grupları tespit edilecektir. Her grup kendi içinde detaylandırılacaktır.

3.2. Varlık gruplarının kritiklik seviyesi belirlenecektir.

Varlıkların kritiklik seviyesinin belirlenmesi için Rehber'in EK-C.1'inde yer alan anket formu kullanılacaktır. Form, her bir varlık grubuna ayrı ayrı uygulanacaktır. Anketlerin uygulanmasında Delfi Metodu kullanılacaktır. İşlenen veriler gizlilik, bütünlük ve erişebilirlik boyutları ile etki alanları (bağımlı varlıklar, etkilenen kişi sayısı, kurumsal sonuçlar, sektörel etki ve toplumsal sonuçlar) boyutları itibariyle değerlendirilecektir. Rehber'in EK-C.2'sinde yer alan form oluşturulacaktır.

3.2.1. Varlıkların kritiklik seviyesini belirlemek üzere Kurum bünyesinde oluşturulacak bir ekiple müşterek çalışılacaktır.

3.2.2. Varlıkların kritiklik seviyesini belirlemek dahil tüm süreçlerde görevlendirilecek Kurum ekibine Bilgi Güvenliği Farkındalığı ve Rehber Uyum Çalışmaları eğitimi verilecektir.

3.2.2.1. Bilgi Güvenliği Farkındalığı eğitiminin içerik ve kapsamı (uygunluğu ve yeterliliği) Kurum tarafından onaylanacak ve özelleştirilebilecektir.

3.3. Mevcut durum ve boşluk analizleri gerçekleştirilecektir.

Bu aşamada Rehber'de yer alan güvenlik tedbirlerinin kurumda fiilen uygulanıp uygulanmadığı tespit edilecek ve uygulanması için yapılması gereken faaliyetler tüm teknik ve süreç detayları ile belirlenecektir. Bu işlem için Rehber'de yer alan güvenlik tedbirlerinin, daha önceki safhalarda belirlenen ilgili varlık grupları ile eşleştirilmesi ve varlıklara özgü soru listeleri (EK-C.3 Mevcut Durum ve Boşluk Analiz Formları) oluşturulması gerekmektedir.

3.3.1. Yüklenici, Kurum'un tefrik edeceği personeli mevcut durum ve boşluk analizleri konusunda eğitecek, müstakil çalışabilecekleri seviyede yetkinlik kazanmalarını temin edecektir. Ayrıca bu çalışmalarda kullanılabilecek yazılımlar konusunda bilgilendirme ve teknik danışmanlık sağlayacaktır.

3.3.2. Yüklenici, mevcut durumun belirlenmesi aşamasında ihtiyaç duyulan güvenlik denetimlerini (sızma testi vb.) yapacaktır. Bu süreçte Yüklenici siber sızma testi, kaynak kod analizi, fiziki güvenlik ve fiziki sızma testi (kurumsal casusluk) konularında uzman personelini hazır bulundurmalıdır.

3.4. Rehber Uygulama Yol Haritası hazırlanacaktır.

Yukarıdaki iş ve işlemler sonucunda ortaya çıkacak olan duruma göre Rehber'de belirtilen tedbirlerin nasıl uygulanabileceğine ve uygulama sürecine (eylem planı) ilişkin yol haritası belirlenerek dokümante edilecektir. Bu doküman yetkinlik kazanımı ve eğitimler, ürün tedariki, hizmet alımı, danışmanlık, geliştirme, tasarlama, sıkılaştırma tedbirleri, sürüm güncelleme, dokümantasyon, kurumsal süreç iyileştirme vb. hususları kapsayabilecektir. Rehber'in EK-C.4 ve EK-C.5 formları oluşturulacaktır.

3.4.1. Tüm çalışmalar (politika, prosedür, talimat vb. dokümantasyon işleri dahil) Kurum bünyesinde ayrıca uygulanması düşünülen ISO27001:2013 Bilgi Güvenliği Yönetim Sistemi (BGYS) standartları göz önünde bulundurularak yürütülecektir.

3.5. Rehber uygulama yol haritasının hayata geçirilmesinin, kontrol edilmesinin yönetimi ve bilgilendirmesi sağlanacaktır.

Kurum'un Rehber uygulama yol haritasını hayata geçirmesinin, kritiklik derecelerine göre sırası ile tedbirlerin uygulamasının, rehber uygulama yol haritasınının kontrol edilmesinin yönetimi ve bilgilendirmesi sağlanacaktır. Bilgi ve iletişim güvenliği denetimi için Kurum'a bilgilendirme sağlanacaktır.