ISO27001 Sertifikasyonu - Bilgi ve İletişim Güvenliği Rehberine Uyum Danışmanlık Hizmeti İhalesi Teknik Şartname

İşin çeşidi : ISO27001 Sertifikası Yenileme / Bilgi ve İletişim Güvenliği Rehberine Uyum Danışmanlık Hizmeti

İşin niteliği :

- ISO27001 sertifikasının güncel versiyonuyla yenilenmesi, gerekli koşulların hazırlanması
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin yayımladığı Bilgi ve İletişim Güvenliği Rehberi'ne uyum çalışmalarının yürütülmesi

konularında yetkin bir firmadan Dış Kaynaklı Bilgi Güvenliği Hizmeti alınması

İşin süresi : 12 (oniki) aydır.

Şartnamede;

İstanbul Bilgi Üniversitesi – BİLGİ,
Santral Kampüsü, Bilişim Teknolojileri Departmanı – BT Dept.
Teklif veren kuruluş – FİRMA
Satın alınacak Donanım / Yazılım / Hizmet ÜRÜN olarak anılacaktır.

ÖN KOŞULLAR

- İşbu şartname,
  - ISO27001 sertifikasının 2022 versiyonuyla yenilenmesi süreçlerinin yürütülmesi, gerekleri için analizlerin yapılması, altyapı ihtiyaçlarının belirlenmesi, planlanması, sertifika yenilemesi ilgili koşulların hazırlanması
  - BİLGİ'nin T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yayınladığı Bilgi ve İletişim Güvenliği Rehberine uyumu, fark analizinin çıkarılması ve kamu sitesine yüklemeye hazır hale getirilmesi, ilerleme planlarının hazırlanması

  konusunda bilgi birikimine sahip olan FİRMA dan danışmanlık hizmeti alımını kapsamaktadır.
- Hizmet alım yeri, BİLGİ' nin Santral Kampusu BT Departmanıdır.
- FİRMA tarafından verilecek hizmet kapsamında, öğrenilen bütün bilgiler ÇOK GİZLİ statüsünde olup, hiçbir şekilde 3. şahıslara veya firmalara yazılı veya sözlü olarak aktarılamaz.

GENEL İSTEK VE ÖZELLİKLER

- Çalışma, teklifin kabul edilerek sözleşme imzalanmasını takiben 15 iş günü içerisinde başlatılacaktır.
- Projenin toplamda 1 (bir) yıl sürmesi, FİRMA'nın teklifi ile beraber detaylı proje planını sunması talep edilmektedir.
- FİRMA, teklifi içerisinde her bir adıma ait adam/gün'lere ilişkin planlamayı sunmalıdır.
- FİRMA proje başladığında bir yıllık kapsama ait bir rapor sunacak, aylık olarak ilerlemeleri raporlayacaktır.
- Ayrıca, söz konusu hizmetin anlık olarak izlenebilir bir proje yönetim ürünü üzerinden izlenebilir olmasını sağlayacaktır.

YETKİNLİKLER ve YETERLİLİKLER

Proje Ekibi,

- Proje yöneticisi olacak kişinin ISO 27001 Baş Denetçi, BIGR Denetçi 1-2, CISA (Certified Information System Auditor) ve CISSP (Certified Information Systems Security Professional) sertifikalarının bulunması
- Her bir proje ekip üyesi için ISO 27001 İç Denetçi sertifikasının bulunması
- Proje ekibi içerisinde sıkılaştırma hizmetlerinin verilebilmesi için minimum 1 (bir) kişide TSE Kıdemli sızma

testi uzmanı, GPEN veya OSCP sertifikasına sahip olması
- Üniversitelerde bilgi güvenliği kapsamında danışmanlık hizmetleri vermiş olması
- Sözleşme yapılmasından sonra proje planında, iş paylaşımı değişikliği veya danışmanların değişimi benzer özelliklere ve deneyimlere sahip olmaları
- Danışmanların projedeki görev paylaşımı ve sorumluluk alanlarının net olarak belirtilmesi

gerekmektedir.

FİRMA'nın,

- FİRMA tarafından hizmeti sağlamak ile yükümlü olacak personelin konu hakkında uzmanlığı, geçmiş deneyimleri, sertifikaları ve detaylı CV bilgilerinin teklifle birlikte iletilmesi,
- Belirtilen yetkinliklere sahip en az 2 uzmanı projede görevlendirmesi, uzmanlardan en az birini ilk 6 ay yerinde çalışma şeklinde en az 20 adam/gün, 2. altı ay yerinde veya uzaktan çalışma şeklinde en az 20 adam/gün görevlendirmesi,
- ISO27001, ISO27701, ISO9001 sertifikalarına sahip olması,
- DDO altında bulunan sıkılaştırma çalışmalarının yapılması amacıyla, OSCP veya GPEN sertifikasına sahip sertifikalı çalışanları olması
- Altyapı ihtiyaçlarına destek verebilmesi amacıyla, kendi bünyesinde güvenlik ürünlerinin kurulum veya yönetim tecrübesine sahip çalışanlar bulundurması

gerekmektedir.

AMAÇ

ISO27001 Bilgi Güvenliği Yönetim Sistemi ile Bilgi ve İletişim Güvenliği Rehberi uyumsuzlukları ile karşılaşmamak, herhangi bir cezai yaptırıma düşmemek, yeni versiyon ISO27001 sertifikasına sahip olmak

İÇERİK

- FİRMA tarafından verilecek Dış Kaynaklı Bilgi Güvenliği Hizmeti'ne yazılım/donanım sağlanması, kurulumu ve konfigürasyonu dahil değildir.
- Hizmet kapsamında BİLGİ için aşağıda tanımlanmış olan görevler yerine getirilecek veya BİLGİ de sorumlu kişiler yönlendirilecektir.
- ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi'ne ve Dijital Dönüşüm Ofisi'nin yayınlamış olduğu Bilgi ve İletişim Güvenliği Rehberi'ne uyum konusunda çalışmalar yapacaktır. Sorumlulukları aşağıdakilerle sınırlı olmamak üzere aşağıdaki gibidir.

    - Bilgi güvenliği yapısının kurulum, işleyiş, güncelleme çalışmalarını gerçekleştirmek; etkinliğini ve uygulamanın bilgi güvenliği politikasıyla uyumlu yürütüldüğünü denetlemek,
    - Birim yöneticileriyle ve birim güvenlik sorumluları ile koordinasyonu sağlamak, işleyişe ilişkin izleme ve değerlendirme faaliyetleri yürütmek,
    - Tüm personelin ve yeni işe başlayanların, bilgi güvenliği ile ilgili eğitimleri almalarını sağlamak, bilgi güvenliği ile ilgili bilinç ve duyarlılığı sürekli kılmak için eğitim programları düzenlemek,
    - Belirtilen kapsamlarda BİLGİ içerisinde gerçekleştirilen çalışmaların iç denetimini yapmak, alınması gereken aksiyonların takibi sağlamak,
    - Bilgi güvenliği çalışmalarının çalışanlar tarafından benimsenmiş, kabul görmüş ve kullanılır durumda oldğunu izlemek,
    - Üst yönetime çalışmalarla alakalı konularda düzenli olarak bilgi vermek,
    - İlgili prosedürlerinin oluşturulmasını ve dökümante edilmesini sağlamak,
    - Bilgi güvenliğini etkileyebilecek yeni düzenlemeler, projeler ve değişiklikler ile ilgili gerekli araştırma, planlama ve yönlendirmeyi sağlamak
    - Senede 2 defa tüm ISO27001 ve BIGR süreçlerini yerinde gözden geçirmek, raporlamak,
    - Firewall kurallarının 1 ay boyunca analiz edilmesini sağlamak (FW kurallarının analiz edilmesi, gölgelenmiş kuralların çıkarılması, aktif olmayanların listelenmesi, loglama kapalı olan kuralların çıkarılması)
    - Kişisel verinin bulunduğu alanlara olan erişimler başta olmak üzere, güvenlik altyapısını kontrol etmek,
    - Tedarikçilerden veya müşterilerden gelen bilgi güvenliği taleplerine cevap vermek,

Cumhurbaşkanlığı Bilgi Güvenliği Rehberi Projesi - DETAY

Bu proje, BİLGİ'nin T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yayınladığı Bilgi ve İletişim Güvenliği Rehberi'nin Kritiklik Derecelendirme ve Boşluk Analizi başlığı altında bulunan yapıya uyumlu hale gelmesi için danışmanlık hizmeti alımına ilişkin teknik detaylar ve yapılacak hizmetlerin yer aldığı şartnamedir.

Çalışmalar FİRMA tarafından veya FİRMA yönlendirmesiyle BİLGİ ekibinin de katılımıyla gerçekleştirilecektir. FİRMA, şablon ve örnekler sağlayarak ve bizzat katılarak çalışmalara destek verecektir. Ayrıca, BİLGİ proje ekiplerine hatırlatmaların yapılması ve envantere ilişkin soruların cevaplanması konusunda da FİRMA destek verecektir.

Planlama ve Ön Hazırlık
Bu aşamada, FİRMA aşağıdaki başlıklar üzerinden çalışmalar gerçekleştirilecektir:

- Proje Ekiplerinin Belirlenmesi,
  - Bilgi Teknolojileri Alt Yapısının anlaşılması
  - Proje Takvimlerinin ve Planlarının hazırlanması
  - Mevcut varlık envanteri, risk analizi ve uygulanabilirlik bildirgesi şablonlarının güncellenmesi

1. Varlık Envanteri Çalışması

Bu aşamada bilgi varlığı envanterinin hazırlanması FİRMA tarafından destek verilecektir.

- Varlık envanteri çalışmalarında Bilgi ve İletişim Güvenliği Rehberi'nde belirtilen varlık ana grupları kapsamında çalışmalar gerçekleştirilecektir.
- Varlık envanteri, varlıkların listelenmesi, sahipliklerinin ve emanetçilerin belirlenmesi, varlıklarının gruplandırılması, gruplama sonucu elde edilen varlık gruplarının kritiklik derecelendirmesinin yapılması başlıklarını içerecek ve FİRMA koordinasyonunda BİLGİ ekipleri ile beraber tamamlanacaktır.
- Bu çalışmanın çıktısı olarak varlık envanteri haricinde, varlık grubu bazında Bilgi ve İletişim Güvenliği Rehberi Ek-C.1: Varlık Grubu Kritiklik Derecelendirme Anketi ile Ek-C.2: Varlık Grubu ve Kritiklik Derecesi Tanımlama Formu da doldurulacaktır.

2. Mevcut Durum ve Boşluk Analizi

Mevcut Durum ve Boşluk Analizi çalışmasında; Bilgi ve İletişim Güvenliği Rehberi Bölüm 3, 4 ve 5'te yer alan güvenlik tedbirlerinin hangilerinin uygulanması gerektiğinin belirlenmesi ve belirlenen güvenlik tedbirlerine göre mevcut durumun tespiti çalışması FİRMA tarafndan yapılacaktır. Rehberde tanımlanan güvenlik tedbirleri aşağıda yer alan üç ana başlık altında sınıflandırılmıştır:

Mevcut durumun değerlendirilmesi ve boşluk analizinin gerçekleştirilmesi tamamlanması ile tüm durumun görülebileceği boşluk analizi raporu ile Bilgi ve İletişim Güvenliği Rehberi EK-C.3 formatında varlık grubu özelinde raporlamalar da ek olarak rapora eklenecektir.

Değerlendirmeler, esas olarak BİLGİ personeliyle yapılacak olan görüşmelere ve doküman incelemelerine dayandırılacaktır:

3. Rehber Harita Yol Haritasının Hazırlanması

FİRMA, Rehber Yol Haritasının Hazırlanması konusunda danışmanlık sağlayacaktır. Yol Haritası, 3 ila 24 ay içerisinde yapılması planlanan çalışmalara bir yol haritası oluşturmayı hedeflemektedir. Format olarak, Rehber Uygulama Yol Haritası Belirleme Formu kullanılarak FİRMA tarafından hazırlanacak olan raporda, BİLGİ tarafından belirlenen tedbirlerin telafi edici kontrollerle karşılanmasına karar verilmesi durumunda "Telafi edici kontrol kayıt formlarının" doldurulması FİRMA eşliğinde ve BİLGİ sorumluluğundadır.