İTKİB GENEL SEKRETERLİĞİ

6698 SAYILI KİŞİSEL VERİLERİ KORUMA KANUNUNA UYUMUN

ISO 27001:2013 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE ISO27018 KRİTERLERİ İLE SAĞLANMASI PROJESİ

TEKLİF ALMA ŞARTNAMESİ

İçindekiler

I. Taraflar

İTKİB; Şartname konusu işi yaptıracak İŞVEREN olan İstanbul Tekstil ve Konfeksiyon İhracatçı Birlikleri Genel Sekreterliği'ni **YÜKLENİCİ**; Şartname konusu işi üstlenmek üzere ihaleye katılan tüzel kişiyi ifade eder.

II. İşin Konusu

6698 Sayılı Kişisel Verileri Koruma Kanununa Uyumun ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi ve ISO 27018 kriterleri ile sağlanması projesi kapsamında danışmanlık hizmeti satın alınacaktır.

6698 SAYILI KİŞİSEL VERİLERİ KORUMA KANUNUNA UYUMUN ISO 27001:2013 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE IS027018 KRITERLERİ İLE SAĞLANMASI PROJESİ

Teknik Şartnamesi

2018

Teknik Şartname İçindekiler

1. GENEL

1.1. İHALE KONUSU

1.1.1. 6698 sayılı Kişisel Verileri Koruma Kanunu'na ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi ve ISO 27018 kriterleri ile Uyum için Danışmanlık

1.2. İHALE AMACI

1.2.1. Kişisel Verileri Koruma Kanununa Uyum için Danışmanlık Hizmeti

1.2.1.1. İdare bünyesinde alınan, işlenen, saklanan ve imha edilen her türlü kişisel verinin, ilgili kişinin veri üzerindeki hakları ile birlikte dokümante edilmesi ve kişisel verileri korumaya yönelik sistemin ISO27001:2013 yönetim sistemi ile kurulması.

1.2.2. Bilgi Güvenliği Yönetim Sistemine Uyum için Danışmanlık Hizmeti

1.2.2.1. İdare bünyesindeki her türlü bilişim sistemlerinde işlenen ve saklanan verilerin aşağıdaki başlıklarda güvenlikle ilgili işleri amaçlanmaktadır, Bütünlüğünün korunması (bilginin bozulmadan muhafaza edilmesi), Gizliliğinin sağlanması (bilginin yetkisiz kişilerin eline geçmesinin engellemesi), Erişilebilirliğinin korunması (bilginin kesintisiz bir biçimde kullanıma hazır halde tutulması), Sistem üzerindeki güvenlik olaylarına doğru ve zamanında müdahale edilmesi. Sızma testleriyle idarenin bilişim sistemlerinde olabilecek güvenlik açıklıklarının veya zafiyetlerinin belirlenerek gerekli iyileştirmelerin yapılması ve önlemlerin alınması,

1.2.2.2. Bilgi Güvenliği Yönetim Sisteminin kurulması ile İdarenin bilişim yapısının dünyada bilgi sistemlerinin güvenliği ve etkin yönetiminde uluslararası standartların en önemlisi olan ISO 27001:2013 standardına ISO27018 kriterleri ile uyumlu hale getirilmesi amaçlanmaktadır.

1.3. KAPSAM

1.3.1. Kurum bünyesindeki bütün birimlerin dijital ve basılı ortamda bulunan tüm veri varlıklarına ilişkin kayıtlı ve mevzuat gereği saklanması gereken bilgileri kapsar. İlgili varlıklarda tespit edilen verilere ilişkin 6698 Sayılı KVKK gereklilikleri,

1.3.2. İdarenin bilişim sistemlerinde olabilecek güvenlik açıklıklarının veya zafiyetlerinin belirlenerek gerekli iyileştirmelerin yapılması ve önlemlerin alınması,

1.3.3. İdare bilişim mimarisinin ve tüm yazılımlarının güvenlik açısından analizi, iyileştirilmeye matuf rapor(lar)ın idareye sunulması ve idare tarafından talep edilmesi halinde iyileştirici yazılımlar ve entegrasyon uygulamaları için detaylı tekliflerinin iletilmesi,

1.3.4. Bilişim güvenliği seviyesinin artırılması ve bu seviyenin korunması amacıyla ISO27001:2013 Bilgi Güvenliği Yönetim Sisteminin ISO27018 kriterleri ile kurulması ve İdarenin bilişim yapısının bu standarda uygun hale getirilmesi,

1.3.5. Siber Güvenlik Kurulu Toplantısında kararlaştırılan ve kurulan SOME ekiplerine gerekli eğitimlerin sağlanması için yapılması gereken çalışmaların gerçekleştirilmesi, kurulum, eğitim, danışmanlık, teknik hizmetleri esaslarını kapsamaktadır

1.4. İŞİN SÜRESİ

1.4.1. Sözleşmenin imzalanmasından itibaren 180 takvim günü içinde analiz ve raporlama işleri tamamlanacaktır.

1.5. FİRMA YETKİNLİĞİ

1.5.1. Firma bünyesinde belgelendirme kurumlarında baş denetçi olarak görev alan ISO27001:2013 Baş Denetçi bulunuyor olması,

1.5.2. Firma bünyesinde CISSP, TSE Ağ ve Sistem Altyapısı Sızma Uzmanı, OSCP, ISO 27001 Baş Denetçi ve CEH, CISA, Endüstri ve İşletme Yöneticiliği sertifikalı personeller bulunması,

1.5.3. Yüklenici ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi Danışmanlık Hizmeti konusunda en az 50 Personeli olan en az 1 firmada danışmanlık hizmeti vermiş veya danışmanlık hizmeti vermek için sözleşme imzalamış olması,

Yüklenici firmanın danışmanlarında en az 5 senelik ISO27001 ve Bilgi Güvenliği yöneticisi pozisyonunda tecrübe sahibi olması,

Tercih sebebidir.

1.6. KISALTMALAR

İDARE	İTKİB
İSTEKLİ	Teklif Sahibi
YÜKLENİCİ	İşi Üstlenen Firma
CISSP	Certified Information Systems Security Professional
CEH	Certified Ethical Hacker
DF	Düzeltici Faaliyet
DPO	Data Protector Officer
GDPR	General Data Protection Regulation
KVKK	Kişisel Verileri Koruma Kanunu

KVKS	Kişisel Verileri Koruma Sistemi
MED	Mahremiyet Etki Değerlendirmesi
PIA	Privacy Impact Assessment
YGG	Yönetimin Gözden Geçirmesi

2. DANIŞMANLIK

2.1. GENEL

2.1.1. Kurum bünyesinde Kişisel Veri ile ilgili bir ekip oluşturulacaktır.

2.1.2. Yüklenici; Bilgi Güvenliği Yönetim Sistemi Kurulumu, ISO 27001:2013 Sertifikasyon Hazırlık Çalışmaları, Zafiyet ve Sızma Testi Çalışmaları, Güvenlik Seviyesi Arttırılması, Sıkılaştırma, Koruma ve Raporlama, Saldırı Sonrası Analizi ve Raporlaması, ISO 27001 Risk Analizi ve Değerlendirmesi, Risk Tedavi Planı ve Uygulanabilirlik Bildirgesinin Hazırlanması, ISO 27001 Sertifikasyon Denetimi öncesi ve sonrası gerekli dokümantasyon ve danışmanlığın sağlanmasından sorumlu olacaktır.

2.1.3. İdare adına Bilgi Güvenliği, ISO 27001 çalışmaları ve KVKK süreçleri Bilgi İşlem Şubesi tarafından yönetilir ve yürütülür.

2.2. KVKK KURULUM ve DANIŞMANLIK ÇALIŞMALARI

2.2.1. KVKS için gerekli rehber dokümanlar hazırlanacaktır.

2.2.2. Hukuki analiz yapılacaktır. Kurum iş sözleşmeleri, üçüncü taraf sözleşmeleri ve genel ve sektörel kurum mevzuatı KVKK açısından incelenerek uyum sağlayıcı revizyonların yapılması sağlanacaktır.

2.2.3. Kurumda yönetim sistemi olarak kanuna uyum sağlamak için gerekecek politika, prosedür ve diğer dokümanlar (Veri koruma, silme, imha, anonimleştirme vb.) hazırlanacaktır.

2.2.4. 10.03.2018 tarihli 30356 sayılı Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliği dikkate alarak 6698 sayılı KVKK'nın 11. Maddesinin kendisine verdiği hakkı kullanmak isteyen ilgili kişilere süresinde cevap vermek üzere İlgili Kişi Yardım Masası kurulması için gerekli öneriler raporu hazırlanacaktır.

2.2.5. Kurumun var olan yazılı hizmet süreçleri incelenerek süreçlerdeki kişisel veriler tespit edilecek ve veri envanteri listesi oluşturulacaktır.

2.2.6. Kurum Dosya Sunucusu üzerindeki dosyalar indekslenerek içlerinde kişisel verileri tespit için tarama yapılacaktır. Tarama ile genel ve özel nitelikli kişisel verilere ulaşılmaya çalışılacaktır. Ayrıca yapılandırılmış verilerin (Veri Tabanları) içindeki kişisel veriler Veri Tespit yazılımları ile analiz edilecektir.

2.2.7. Kişisel verileri ve kritik bilgi varlıklarını dikkate alan bir sınıflandırma

yapılacaktır.

2.2.8. Envanteri çıkartılan verilerin KVKK açısından veri riskleri analizi yapılacaktır.

2.2.9. Kurumda tutulan kişisel verilerin ilgili mevzuat ve/veya oluşturulacak makul çerçeveye göre veri tutma limitleri belirlenecektir.

2.2.10. Veri yaşam döngüsü ve periyodik etkinlikler ile ilgili kurum ihtiyaçları belirlenecektir.

2.2.11. KVKK Uyumunu sağlamak üzere kurgulanacak yapıda bulunması gereken birim/kişi görev tanımları ile ilgili tavsiyeler dokümante edilecektir.

2.2.12. KVKK Uyumunu sağlamak üzere kurgulanacak yapıda bulunması gereken çalışan sözleşmeleri ile ilgili tavsiyeler dokümante edilecektir

2.2.13. KVKK Uyumunu sağlamak üzere kurgulanacak yapıda bulunması gereken veri sorumlusu ve veri işleyen sözleşmeleri, KVKK web sitesinde 15.05.2018 tarihinde yayınlanan "Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurları da dikkate alınarak hazırlanmasına yönelik tavsiyeler dokümante edilecektir.

2.2.14. Envanterdeki verilerin MED- Mahremiyet Etki Değerlendirmesi (PIA Raporu) yapılacaktır.

2.2.15. 10.03.2018 tarihli 30356 sayılı Resmî Gazetede yayınlanan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'e uygun şekilde Aydınlatma, rıza ve vazgeçme beyanları oluşturulacaktır.

2.2.16. Veri alma, kayıt, saklama ve silme operasyonlarının süreçleri incelenecek, gerekli revizyonlar önerilecektir.

2.2.17. Kurumun VERBİS'e kaydı yapılacaktır. KVK kurumu ile iletişim sağlamak için veri sorumlusu irtibat kişisi atanması konusunda danışmanlık verilecektir.

2.2.18. KVKS (Kişisel Veri Koruma Sistemi) için gerekli organizasyon yapısı oluşturulacak ve görev tanımları belirlenecektir.

2.2.19. KVKS'nin sağlıklı bir şekilde kullanılabilmesi ve kişisel verilerin korunabilmesi için gerekli teknoloji önerileri doküman olarak sunulacaktır. Bu kapsamda veri sızıntısı engelleme, veri maskeleme, şifreleme, psödönimleştirme, tokenize etme, anonimleştirme için gerekebilecek teknolojiler incelenecektir.

2.2.20. 28.10.2017 tarihli 2017/30224 sayılı Resmî Gazetede yayınlanan "Kişisel Verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hakkında yönetmelik" şartlarını sağlamaya yönelik öneriler yapılacaktır.

2.2.21. 31.01.2018 tarihli 2018/10 sayılı Resmî Gazetede yayınlanan "Özel Nitelikli Kişisel Verilerin işlenmesinde Veri Sorumlularınca alınması gereken yeterli önlemler" konulu KVKK kararına uygun şekilde Özel Nitelikli Kişisel Verilerin şifreli saklanması ve korunması için gerekli teknoloji ve sistem önerileri

yapılacaktır.

2.2.22. Erişim yetkileri incelenecek, gerekli düzenlemeler önerilecek, kritik ortamların/kişilerin ayrıştırılması sağlanacaktır.

2.2.23. Bulut kullanımı incelenecek, gerekli tavsiyeler sunulacaktır.

2.2.24. Diğer yönetim standartları ile bütünlük arz etmek üzere Doküman ve sistemleri tekilleştirme tavsiyeleri verilecektir.

2.2.25. Kurumdaki "İhlal Yönetimi", "SOME", "İç Denetim" benzeri uygulamaları KVKS'yi besleyecek şekilde düzenleme tavsiyeleri verilecektir.

2.2.26. Proje kapsamında kurumun 5651 yasasına uyumluluğu incelenecek, gerekli tavsiyeler verilecektir.

2.3. ISO 27001:2013 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

2.3.1. ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KURULUMU İŞLEMLERİ

2.3.1.1. İdarenin Bilgi İşlem Şubesi bünyesinde, Kurumun bilgi varlıklarını içerden veya dışarıdan gelebilecek ve kaza ile veya kasten oluşabilecek bütün tehditlere karşı korumak maksadı ile Bilgi Güvenliği Yönetim Sistemi (BGYS) Yüklenici tarafından kurulacak ve çalıştırılacaktır.

2.3.1.2. İdare Bilişim Sistemlerinde uygulanacak güvenlik politikası oluşturularak, güvenlik standartları belirlenecek ve güncel tutulacaktır.

2.3.1.3. Güvenlik politika ve standartlarının uygulanması, uygulatılması, uygulandığının denetlenmesi ve takibinin yapılması sağlanacaktır.

2.3.1.4. Toplantı güvenliğini sağlamaya yönelik prosedürler oluşturulacak, bu prosedürler kritik toplantıların öncesindeki tedbirleri içerecektir.

2.3.1.5. Bilişim Sisteminin her türlü iç ve dış tehdide, yetkisiz erişime ve zararlı kod ve yazılımlara karşı korunmasına yönelik tedbirlerin alınması ve uygulanması sağlanacaktır.

2.3.1.6. Bilişim Sistemi üzerinde uygulanacak güvenlik kontrollerinin planlanmasına, hazırlanmasına ve uygulanmasına ilişkin çalışmaların yönetimi ve uygulanması sağlanarak, uygulandığının denetim ve takibi yapılacaktır.

2.3.1.7. Bilişim Sistemleri içerisinde meydana gelebilecek güvenlik ihlallerine veya bilgisayar güvenlik olaylarına ilişkin veriler toplanarak güvenlik analizi yapılacak ve raporları hazırlanacaktır.

2.3.1.8. Bilişim sisteminde işlenen, kaydedilen ve saklanan verilerin güvenliğinin sağlanması amacıyla Sistem üzerindeki kullanıcı, sunucu, network, uygulama, veri tabanı ve güvenlik donanımlarının güncel (log) kayıtları toplanıp takip ve analizi yapılacaktır.

2.3.1.9. Bilişim Sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmaları yapılacaktır.

2.3.1.10. Yüklenici, yukarıda belirtilen Bilgi Güvenliği ve ISO 27001 Çalışmaları kapsamında gerçekleştirilecek faaliyetleri yürütmek üzere; İdare için oluşturduğu diğer ekip personeli ve/veya tahsis ettiği diğer personel haricinde, hazırlık süresince (sertifikasyon denetimine kadar), Bilgi Güvenliği ve ISO 27001 Çalışmaları Ekibi oluşturacaktır. Proje ekibinde yukarıda belirtilen niteliklerde 1 (bir) Proje Yöneticisi ve proje yöneticisinin uygun gördüğü miktarda ekip çalışanı olacaktır.

2.3.1.11. Yüklenici, sözleşme süresince; 1 (bir) personelini Proje Yöneticisi olarak atamak, Bilgi Güvenliği ve ISO 27001 Çalışmaları başta olmak üzere, Sistem Yönetimi ve Bilişim Ağları, Donanım ve Teknik Destek Hizmetleri faaliyetleri ile ilgili tüm süreçlerde İdarenin muhatap kabul edebileceği, sorumlu tek isim olarak bildirmekle yükümlüdür.

2.3.1.12. Yüklenici, ISO 27001 sertifikasyon denetimine kadar; yukarıda verilen İdare envanteri ve İdarenin belirleyeceği periyodlarda gerçekleştireceği analiz çalışması sonuçları doğrultusunda oluşturacağı, İdare tarafından onaylanan "Aylık Bilgi Güvenliği ve ISO 27001 Çalışmaları Faaliyet ve Bakım Planı" çerçevesinde gerekli olduğu durumlarda Bilgi Güvenliği Uzmanını İdareye tahsis edecektir. Yüklenici, söz konusu personel ile asgari düzeyde iş bu teknik şartname kapsamında belirtilen ve/veya İdare'nin belirttiği faaliyetleri gerçekleştirecek ve Bilgi Güvenliği Yönetim Sisteminin işletilmesinden sorumlu olacaktır.

2.3.1.13. Yüklenici, ISO 27001 sertifikasyon denetiminden önce; 2 (iki) ay boyunca; yukarıda verilen İdare envanteri ve İdare'nin belirleyeceği periyodlarda gerçekleştireceği analiz çalışması sonuçları doğrultusunda oluşturacağı, İdare tarafından onaylanan "Aylık Bilgi Güvenliği ve ISO 27001 Çalışmaları Faaliyet ve Bakım Planı" başta olmak üzere; Sistem Yönetimi ve Bilişim Ağları, Donanım ve Teknik Destek Hizmetleri faaliyetleri çerçevesinde, resmi iş günlerinde haftada en az 1 (bir) tam gün olarak, en az 1 (bir) Bilgi Güvenliği Uzmanını İdare'ye tahsis edecektir. Yüklenici, söz konusu personel ile asgari düzeyde işbu teknik şartname kapsamında belirtilen ve/veya İdare'nin belirttiği faaliyetleri gerçekleştirecek ve Bilgi Güvenliği Yönetim Sisteminin Test Faaliyetlerinin işletilmesinden sorumlu olacaktır.

2.3.1.14. Bilgi Güvenliği ve ISO 27001 çalışmaları faaliyet günlerinin resmî tatillere denk gelmesi durumunda İdare onayı alınarak bakım faaliyeti bir sonraki resmi iş günü içerisinde gerçekleştirilecektir.

2.3.1.15. İdare'nin, sözleşme süresi içinde toplamda 30 saati aşmamak üzere Yüklenici Bilgi Güvenliği ve ISO 27001 Çalışmaları Ekibi personeline resmi iş günleri haricinde ve mesai saatleri dışında da bazı çalışmaları veya müdahaleleri gerçekleştirmesi gereken talepleri olabilecektir. Bu talepler doğrultusunda Yüklenici Bilgi Güvenliği ve ISO 27001 Çalışmaları Ekibi personeli gerekli çalışmaları veya müdahaleleri İdare'nin talep ettiği zamanda ve sürelerde yapmakla yükümlüdür.

2.3.2. ISO 27001 SERTİFİKASYON ÇALIŞMALARI

2.3.2.1. İdare sistem merkezinden sağlanan bilişim hizmetleri için ISO 27001 standartlarının sağlanması ve bilişim hizmetlerinin ISO 27001 standartları gerekleri doğrultusunda yürütülmesi, bu kapsamda İdare sistem merkezinden yönetilen bilişim hizmetleri odağında Türk Akreditasyon Kurumu'ndan akredite ISO 27001 sertifikasının temin edilmesi gerekmektedir. Bu kapsamda asgari düzeyde Yüklenicinin sağlaması gerekenler aşağıda ifade edilmiştir.

2.3.2.2. ISO 27001'de tanımlanmış olan ISMS (Information Security Management System) iş süreçlerinin Kurumun Bilgi Teknolojileri Bölümü içerisinde uygulanması sağlanacaktır ve gerekebilecek muhtemel teknolojik iyileştirmelerin önerilecektir.

2.3.2.3. ISMS politikası oluşturulacaktır. Bu politika Kurum bilgi güvenliği prensipleri, iş ve yasal gereksinimler, risk yapısı dikkate alınarak oluşturulmalıdır.

2.3.2.4. Kurum içi risk analizi yapılacaktır. Risk analizi yapılması sırasında aşağıda belirtilen testler ve çalışmalar gerçekleştirilmelidir:

2.3.2.4.1. Teknik Güvenlik Testleri,

2.3.2.4.2. Kavramsal Güvenlik Testleri,

2.3.2.4.3. Anketler ile Kapsam ve Süreçlerin Belirlenmesi

2.3.2.5. Teknik güvenlik testlerinde iç penetrasyon denemeleri ve/veya testleri, dış penetrasyon denemeleri ve/veya testleri, güvenlik testleri ve/veya taramaları yapılacaktır. Kurum bilgisayarları ilgili testlerden ve/veya taramalardan geçirilecektir.

2.3.2.6. Analiz sonucu tespit edilen güvenlik olaylarıyla ilgili gerekli iyileştirici, düzenleyici ve önleyici çalışmalar Yüklenici tarafından koordine edilecek ve gerçekleştirilecektir.

2.3.2.7. Yapılmış olan testler sonucunda teknik test raporu, yönetimsel test raporu, kavramsal güvenlik test raporu ve anketler oluşturularak Kuruma teslim edilecektir.

2.3.2.8. Oluşturulmuş olan teknik test raporu, yönetimsel test raporu, kavramsal güvenlik test raporu ve anketler ile risk analizi gerçekleştirilecektir.

2.3.2.9. İş sürekliliği planı, risk tedavisi dokümanı, güvenlik politikası, acil durum eylem planı, kullanıcı adı ve şifre politikası Yüklenici tarafından oluşturulacaktır.

2.3.2.10. Risk analizi kapsamında Bilgi Teknolojileri ile ilişki içerisinde olan iş süreçleri analiz edilecektir.

2.3.2.11. Risk analizi sonucunda risk tedavi planı oluşturulacak ve oluşturulmuş

olan bu planın uygulanması sağlanacaktır. Bu kapsamda hangi risklere ilişkin önlemler alınacağı ve hangi risklerin kabul edileceği tanımlanacaktır.

2.3.2.12. Çalışma sürecinde Kurum tarafından yapılması gerekebilecek çalışmalar belirlenecek ve ilgili çalışmalar sürece dâhil edilerek gerekli planlama yapılacaktır. Sürecin ilerlemesi Yüklenici tarafından koordine edilecektir. Yapılan çalışmaların ISMS süreçlerine uygun olarak yapılması Yüklenici sorumluluğundadır.

2.3.2.13. Çalışmanın ardından ISMS yapısının geliştirilmesi için yapılması gerekenler ayrıntılı olarak belirtilmelidir.

2.3.2.14. Kurum bilgi işlemi içerisinde kullanılması gereken operasyon prosedürleri belirlenecek ve yazımı sağlanacaktır. Bu prosedürlerin Kurum içerisinde uygulanması için gerekli koordinasyon gerçekleştirilecektir. Gözden geçirilmesi veya yazılması beklenen başlıca prosedürler şunlardır:

2.3.2.14.1. Personel Planlama Dokümanı

2.3.2.14.2. Personel Sorumlulukları Dokümanı

2.3.2.14.3. İç Denetim Esasları Dokümanı

2.3.2.14.4. İrtibat Listesi Dokümanı

2.3.2.14.5. Firmalarla yapılacak Gizlilik Anlaşması Dokümanı

2.3.2.14.6. Kişilerle yapılacak Gizlilik Anlaşması Dokümanı

2.3.2.14.7. Dış Bağlantı Güvenliği Esasları

2.3.2.14.8. Varlık Sınıflandırma Esasları

2.3.2.14.9. Kullanıcı Eğitim Dokümanı

2.3.2.14.10. BT Sistem Odası Güvenlik Esasları

2.3.2.14.11. Ağ Altyapısı Standartları

2.3.2.14.12. Kullanıcı kimliği ve e-posta tanımlama esasları

2.3.2.14.13. İşletim Sistemleri Güvenlik Kuralları

2.3.2.14.14. Internet Erişim Kuralları

2.3.2.14.15. Kullanıcı Bilgilendirme Kuralları

2.3.2.14.16. Dizüstü Bilgisayar Kullanımı ve Güvenliği

2.3.2.14.17. Veri Depolama Sistemi Kuralları

2.3.2.14.18. Yedekleme Sistemi Yapısı

2.3.2.14.19. Yedekten Geri Dönüş Esasları

2.3.2.14.20. Bilgisayar Elden Çıkarma Esasları

2.3.2.14.21. Veri tabanı Yedekleme ve Bakım Esasları

2.3.2.14.22. Virüs ve Zararlı Yazılımlardan Korunma Esasları

2.3.2.14.23. Windows Makineleri Güvenlik Esasları

2.3.2.14.24. Yazılım Kurulumu Esasları

2.3.2.14.25. Personel İlişik Kesme Esasları

2.3.2.14.26. Kullanıcı Bilgisayarları Kurulum ve Kullanım Esasları

2.3.2.15. Sistemlerde uygulanması gereken güvenlik konfigürasyonları belirlendikten sonra bu esasların sistemde uygulanması için gerekli konfigürasyonlar Yüklenici tarafından gerçekleştirilmelidir.

2.3.2.16. İstekli Bilgi varlıkları envanterinin oluşturulmasını sağlamalıdır. Hazırlanan envanterin ISO 27001 sertifikasyonu için uygunluğunu sağlamak amacı ile, bilgi varlığı envanterinin oluşturulması ve sınıflandırılmasının eksiksiz olarak yapıldığının belirleyebilmek için İdare içinde yer alan varlık sahipleri ile görüşülecektir. Bu görüşmeler sonrasında iyileştirilme ve güncelleme önerileri getirebilecektir.

2.3.2.17. Oluşturulan envanter listesi ISO 27001 Risk Analizine ve gerçekleştirilecek zafiyet testlerinin araç ve metot tayinine bir girdi teşkil edecektir.

2.3.2.18. Oluşturulan varlık envanterinin sürekliliğinin sağlanması ve yönetimi için gerekli belgeler (politika, prosedür, talimat, form, vs.) Yüklenici tarafından hazırlanacaktır. Bu belgelerin hazırlanması hususunda Yüklenici, BGYS Ekibini yönlendirilecek ve danışmanlık hizmeti verecek, gerekli görülmesi durumunda da örnek belge sağlayacaktır.

2.3.2.19. İlgili prosedürlerin teslim edilmesi, risk analizinin yapılması, uygulama planının oluşturulması ve uygulanabilirlik bildirgesinin tesliminden sonra ISO 27001 sertifikasının alınması için İdarece TÜRKAK'dan akredite bir belgelendirme kuruluşuna başvuru yapılacaktır.

2.3.2.20. Yüklenici, yapması gereken tüm çalışmaları, (gerekli bilgilerin oluşturulması) kurum proje yetkilileri ile koordine sağlayarak tamamlayacak ve çalışma raporlarını 140 gün içerisinde İdareye yazılı olarak teslim edecektir. Bu aşamadan sonra İdare, ISO 27001 sertifikasının alınması için gerekli başvuruları yapacaktır. Sertifika denetim süreci sonrasında da Belgelendirme Kuruluşunun Kurumu ziyareti esnasında firma yetkili teknik elemanı Kurum yetkili personeli ile birlikte çalışacaktır. Bu sertifikanın alınamaması halinde yeterli altyapı çalışması yapılmadığı kabul edilecek ve Yüklenici, İdarenin gerekli gördüğü konularda yeniden çalışma yapacaktır. Bu durum sertifikanın alınmasına kadar devam edecektir. Sertifikanın ilk

denetlemede alınamaması halinde Belgelendirme Kuruluşuna yapılacak tüm ödemeler Yüklenici tarafından karşılanacaktır. İşin başlangıcından sertifika alım tarihine kadar geçecek süre 180 günü aşmayacaktır. Planlanmayan olumsuzluklar nedeniyle, proje anılan süreyi aşarsa Yüklenici bu durumu ayrıntılı rapor ile Kurumumuza sunacaktır.

2.3.3. BİLİŞİM GÜVENLİĞİ TESTLERİ

2.3.3.1. Teklif sunacak firma veya Altyüklenici firmanın konusunda en az 2 yıllık tecrübesinin olması

2.3.3.2. Sızma testleri kapsamında minimum Aktif Cihazlar, Bilişim Güvenlik Sistemleri ve Sunucu Altyapısı testleri, DNS Servisleri testleri, Etki Alanı Sunucusu testleri, E-posta Sunucusu testleri, Veri tabanı Sistemleri testleri, Web Uygulamaları testleri, Kablosuz Ağ Sistemleri testleri, Sosyal Mühendislik Testleri, Otomasyon Yazılım Sunucuları testleri yapılacaktır.

2.3.3.3. Yüklenici, denetimi gerçekleştirecek uzmanları açık özgeçmişleri ve projede alacakları görevleriyle birlikte tanıtacaktır.

2.3.3.4. Güvenlik Denetimi kurumun merkez yerel ağ (LAN) sistemleri üzerinden, bir adet uzak birimden ve Internet üzerinden gerçekleştirilecektir.

2.3.3.5. Kurumun domain ve subnetlerinde, internet üzerinden erişilebilir bilinen IP adres aralığında çalışan sunucularındaki güvenlik açıkları taranacak ve bunların oluşturduğu güvenlik açıkları ve riskler tespit edilecektir.

2.3.3.6. Internet'e açık çalışan sunucular üzerinde çalışan web uygulamalarının güvenliği denetlenecektir.

2.3.3.7. Sunucular ile ilgili açık portlar, kullanılan uygulamalar ve uygulamaların olası güvenlik açıkları kontrol edilecektir. (VM, Mail, AD, DB vb. tüm sunucular)

2.3.3.8. Ağ trafiği belli noktalardan izlenecek, trafik kaynakları ve protokoller belirlenecek, olası saldırı imzaları raporlanacaktır.

2.3.3.9. Firewall-İç Network arasında izleme yapılacaktır.

2.3.3.10. Aktif network cihazlarında güvenlik açıklarına karşı tarama yapılacaktır. (Merkez bina omurga network cihazları)

2.3.3.11. Lokasyonların güvenliğinin belirlenmesi ve lokasyonlardan hangi servislere erişilebildiğinin testi için lokasyonlardan birinde güvenlik açığı kontrolleri yapılacaktır.

2.3.3.12. Merkezdeki omurga aktif network cihazlarının ve firewall cihazlarının konfigürasyon kontrolleri yapılacaktır.

2.3.3.13. Web sayfasının dışarıdan erişimlerde güvenlik açıklarının olup olmadığının kontrolü yapılacaktır.

2.3.3.14. Veri tabanı güvenlik analizi ürünü ile detaylı veri tabanı güvenlik analizi yapılacaktır.

2.3.3.15. Yapılan analizlerin sonucunda formatı Güvenlik Denetim Raporu hazırlanarak, bulunan güvenlik açıklarının ne gibi risklere sebep olduğu belirtilecektir. Raporda, bulunan açıklara karşı alınacak önlemler ile güvenliği arttırmak için gerekli iyileştirici öneriler yer alacak, sistemde tespit edilen güvenlik açıklarının taşıdıkları riskler itibariyle öncelikleri ve giderilmesi için yapılması gereken işlemler detaylı ve anlaşılır bir şekilde tarif edilecektir. Rapor Türkçe olacaktır.

2.3.3.16. Kurum çalışanlarının bilgi güvenliği farkındalıklarının sınanması amacıyla kurumdan alınacak bir mail listesine kandırma maili denemesi yapılacaktır (sosyal mühendislik testi).

2.3.4. GÜVENLİK SEVİYE ARTTIRILMASI, KORUMA, RAPORLAMA

2.3.4.1. Yüklenici İdarenin BT altyapısında yer alan fiziksel ve sanal sunucu ile birlikte ağ cihazları için güvenlik ve yama önerilerini iletecektir.

2.3.4.2. Sunucu ve ağ sistemleri ile ilgili kritik sistemler belirlenerek felaket anında neler yapılacağı, nasıl kurtarılacağı ile ilgili analiz yapılacak, rapor halinde sunulacaktır.

2.3.4.3. Yama ve güncellemelerin sağlıklı bir şekilde takip edilmesi ve atlanmadan yapılması için gerekli sistem önerilecektir.

2.3.4.4. Sistemden çıkartılan veya farklı bir sistemde/kişide değerlendirilecek olan donanımların içindeki bilgilerin kalıcı bir şekilde silinmesi için gerekli sistem önerilecektir.

2.3.4.5. Sıfır gün (zero-day) saldırıları tespit edebilmek için kullanılabilecek çözümler önerilecektir.

2.3.4.6. Mobil cihazların ve cihazlardaki verilerin güvenliğinin sağlanması için gerekli sistem önerilecektir.

2.3.4.7. Bina giriş çıkışlarda kullanılan sistemlerin güvenliği ile ilgili analiz yapılacak ve raporlanacaktır.

2.3.4.8. Ağ cihazları ve sunucular üzerinde çalışan gereksiz hizmetler ve servis yazılımları tespit edilecek ve İdare ile mutabık kalınması durumunda kapatılması sağlanacaktır.

2.3.4.9. Etki alanı ve erişim mimarisi incelenerek, tek kullanıcı adı ve şifre ile farklı sistemlere erişim sağlanabilmesi (single-sign-on) için yapılması gerekenler raporlanacaktır.

2.3.4.10. Sunucu ve ağ cihazları sıkılaştırma çalışmasının temel faaliyeti olarak "Center for Internet Security (CIS)" tarafından tanımlanan güvenlik standartlarının Windows ve Linux ve Unix sunucu sistemleri için uygulandığı gösterilecektir.

2.3.5. ISO 27001 RİSK ANALİZİ ve DEĞERLENDİRMESİ

2.3.5.1. Tehdit, zafiyet, risk ve uygulanacak kontrollerin tespitinde ISO 27001 Standardı maddelerinin tümü göz önüne alınacaktır.

2.3.5.2. Bu aşama sonunda, İdare tarafından hazırlanmış olan taslak Risk Değerleme Yöntemi belgesi, Yüklenici tarafından ISO 27001 standardına uyum açısından kontrol edilecektir ve son haline getirilecektir.

2.3.5.3. Buna ek olarak, İdare tarafından hazırlanmış olan aşağıda belirtilen taslak aşamasındaki belgeler de Yüklenici tarafından ISO 27001 standardına uyum açısından kontrol edilecektir ve son haline getirilecektir.

2.3.5.3.1. Risk Yönetimi Politikası

2.3.5.3.2. Risk Yönetimi Prosedürü

2.3.5.3.3. Risk Yönetimi Kılavuzu

2.3.5.4. İstekli ile beraber İdare tarafından aşağıdaki iş adımlarına göre risk analizi gerçekleştirilecektir:

2.3.5.4.1. Varlık değerleme metodu belirlenecektir.

2.3.5.4.2. Tehdit ve zafiyet analizi için Zafiyet ve Sızma Testleri sonuçları da (sadece bu zafiyetler kaynaklı tehditler yeterli değildir) zafiyet tehdit listesinin oluşturulmasına temel teşkil edecektir.

2.3.5.4.3. Tehdit ve zafiyet analizinde, İstekli tarafından yapılan bilgi sahipleri ve/veya ilgiler ile yüz yüze görüşmeler zafiyet ve tehdit listesinin oluşturulmasına katkı verecektir.

2.3.5.5. En az aşağıdaki etki alanlarını da içeren tehdit ve zafiyet analizi yapılacaktır.

2.3.5.5.1. Dış kurum, kişiler ve paydaşlardan gelecek tehditler

2.3.5.5.2. Bilişim sistem operasyonları ve işletmesinden kaynaklanacak tehditler

2.3.5.5.3. Bilişim eleman ve kullanıcılarından gelecek tehditler

2.3.5.5.4. Organizasyon ve iş sorumluluklarından gelecek tehditler

2.3.5.5.5. Yazılım geliştirme ortamlarından gelebilecek tehditler

2.3.5.5.6. Bilişim ağ ve sunucu sistem yönetim işlevlerinden gelebilecek tehditler

2.3.5.5.7. Fiziksel ve mantıksal erişim tehditleri

2.3.5.5.8. Doğal koşul ve felaketlerden gelecek tehditler

2.3.5.5.9. Tehdidin bilgi varlığını etkileme şiddeti tespit edilecektir. Tehdidin risk faktörü hesaplanacaktır.

2.3.5.5.10. Riskin önem derecesi tespit edilecektir

2.3.5.5.11. Kabul edilebilir ve kabul edilemez önem derecelerindeki yöntemleri tespit edilecektir.

2.3.5.5.12. Her tehdit ve zafiyete karşılık gelen mevcut güvenlik önlemleri belirlenecektir.

2.3.5.5.13. Risk analizi tablosu oluşturulacaktır. Oluşturulacak elektronik risk analizi tablosu en az aşağıdaki alanlardan oluşacaktır.

- Sıra No
- Varlık
- Varlığın Sonuç Değeri
- Tehdit
- Zafiyet
- Mevcut Kontroller
- Tehdidin Oluşma Olasılığı
- Tehdidin Hasar Derecesi
- Hesaplanan Risk değeri
- İlave Kontroller
- Kontroller Sonrası Tehdidin Oluşma Olasılığı
- Kontroller Sonrası Tehdidin Hasar Derecesi
- İndirgenmiş Risk Değeri

2.3.5.5.14. İstekli, "Kabul Edilebilir Riskler" için kullanılacak yöntemler önerecek ve İdare bu önerileri değerlendirerek yöntemleri belirleyecektir.

2.3.6. RİSK TEDAVİ PLANI ve UYGULANABİLİRLİK BİLDİRGESİ HAZIRLANMASI

2.3.6.1. Risk analizi ve değerlendirmesi çalışması sonucunda tespit edilen her risk için mevcut güvenlik kontrollerine ek güvenlik önlemleri İstekli tarafından önerilecektir. Önerilen ek güvenlik kontrollerinin uygulanmasının kısa gerekçeleri belirlenecektir. Önerilen ek güvenlik kontrolleri teknik, idari, fiziksel konuları içerebilecektir. Bu aşama sonunda, İdare onaylanan ek güvenlik önlemleri uygulanarak, hazırlanan Risk Analizi tablosu ek güvenlik önlemleri, ilgili kontrolün sorumlusu, başlangıç bitiş tarihleri ve maliyet alanları eklenecek ve nihai olarak Risk Tedavi Planı Tablosu oluşturulacaktır.

2.3.6.2. Risk Analizi ve Risk Tedavi Planı Tabloları oluşturulduktan sonra

Uygulanabilirlik Bildirgesi (SOA Tablosu) ISO27018 kriterleri ile hazırlanacaktır. Bu tablo en az aşağıdaki başlıkları içerecek şekilde

2.3.6.2.1. ISO 27001 Kontrol Konusu

2.3.6.2.2. ISO 27001 Kontrol Maddesi

2.3.6.2.3. Uygulanıp uygulanmadığı

2.3.6.2.4. Referans dokümanı (Oluşturulacak dokümanlarda da yer gösterilecektir)

2.3.7. SİBER OLAYLARA MÜDAHALE EKİBİ (SOME) DANIŞMANLIĞI

2.3.7.1. SOME sorumlukları belirlenecek ve ekip görev listesi hazırlanacak, SOME kapsamında gerekli dokümantasyon (prosedürler vs.) hazırlanacaktır.

2.3.7.2. İdare bünyesinde etkin bir Siber Olaylara Müdahale Ekibi (SOME) kurulacak ve SOME'nin USOM kaydı işlemleri Yüklenici tarafından gerçekleştirilecektir. SOME eğitimlerinden sonra Kurumsal SOME ekibi çalışmalarına yıl sonuna kadar destek olmak amacıyla bir güvenlik uzmanını görevlendirilecektir. Eğitimleri sağlayacak personel en az 4 yıllık üniversite mezunu ve ISO27001 baş denetçi sertifikası sahibi olacaktır.

2.4. PROJE EKİBİ

2.4.1. Proje ekibi içerisinde üniversitelerin 4 yıllık bölümlerinden mezun, en az birer tane olmak üzere aşağıdaki özelliklerde personel bulunması **tercih sebebidir**. Yüklenici proje ekibi ile ilgili özgeçmiş bilgilerini ihale dosyasında paylaşacaktır;

2.4.1.1. Bir üniversite eğitim program neticesinde alınmış proje yöneticisi belgesi olmalı

2.4.1.2. Uluslararası geçerliliği olan ISO 27001 Lead Auditor (Baş Denetçi) sertifikasına sahip, akredite denetim kuruluşlarında Baş Denetçi olarak çalışan olmalı,

2.4.1.3. Daha önce en az bir 6698 sayılı KVKK kanununa uyum projesinde görev almış hukukçu olmalı

2.4.1.4. ISACA (Information Systems Audit and Control Association)'dan alınmış en az 10 yıllık geçmişi olan CISA (Certified Information Systems Auditor) sertifikası olmalı,

2.4.2. BGYS çalışmaları sırasında İdare hakkında edinilebilecek bilgilerin önemi ve gizliliği nedeniyle söz konusu işlemi gerçekleştirecek Yüklenici ile İdare arasında bir gizlilik sözleşmesi düzenlenecektir. Proje ekibi zorunluluk olmadıkça değiştirilmeyecektir

2.4.3. Yüklenici ihale konusu danışmanlık hizmetlerini gerçekleştirirken altyüklenici kullanabilecektir, söz konusu altyüklenicilerin listesini ihale dosyasında paylaşacaktır.

2.5. EĞİTİM

2.5.1. Kurum yöneticilerine ve süreç sorumlularına en az 4 saatlik KVKK Bilinçlendirme ve farkındalık Eğitimi verilecektir.

2.5.2. İlgili kurum çalışanlarına KVKK maksimum 4 oturumda Farkındalık Eğitimi verilecektir.

2.5.3. Yüklenici, İdare'nin belirleyeceği en çok 10 personeline teklif ettiği ve teslim ettiği KVKS Konusunda teknik eğitimi ve uygulama eğitimi İdare'nin belirleyeceği merkezde ücretsiz olarak sağlayacaktır.

2.5.4. Kişisel Veri ihlali yönetim süreci ile ilgili eğitim verilecektir.

2.5.5. Kurumun kanuna sürekli uyumunu sağlamak üzere bir iç denetim kurgusu yapılarak kurumun kendisini denetlemesi için eğitim ve danışmanlık verilecektir.

2.5.6. Kurumun KVK Sisteminin sürdürülebilirliğini sağlamak için gerekli olan test, tatbikat, YGG, İç Denetim ve DF gibi uygulamalar hakkında eğitim verilecektir.

2.5.7. BGYS Konusunda İdarenin Bilgi-İşlem personeline aşağıdaki konuları içeren ve en az 4 saatlik Güvenlik Eğitimi verilecektir. Yüklenici, İdare'nin belirleyeceği en çok 10 personeline teklif ettiği ve teslim ettiği Bilgi Güvenliği Yönetim sistemi Konusunda teknik eğitimi İdare'nin belirleyeceği merkezde ücretsiz olarak sağlayacaktır.

2.5.7.1. ISO 27001:2013 Etki Alanları

2.5.7.2. ISO 27001 Bilgi Güvenliği Politikası ve ekleri

2.5.7.3. Güvenlik tehditleri

2.5.7.4. Risk Değerlendirmesi ve Önlemleri

2.5.8. Gerek ISO 27001 sistemi farkındalığını oluşturmada ve gerekse kurulacak SOME'nin oryantasyonunu sağlamak üzere eğitim verilecektir.

2.5.9. Farkındalık eğitimleri 2 kere, SOME eğitimleri 1 kere Kuruma verilecektir.

2.5.10. Farkındalık artırmaya yönelik posterler kuruma özel tasarlanarak Kuruma tasarım olarak teslim edilecektir. En az 5 farklı poster tasarlanacaktır. Bu posterler Kurum iç mekânda duvarlara asılmaya uygun olacaktır.

2.5.11. Eğitim, tüm Kurum yöneticileri ile Bilgi İşlem departmanının tüm çalışanlarını kapsayacaktır.

2.6. DOKÜMANTASYON

2.6.1. Tüm proje bilgileri İdare'nin onay vereceği bir elektronik formatta dokümante edilerek İdare'ye teslim edilecektir. Dokümanların kabulü için İdare'den onay alınacaktır.

III. Tekliflerin Veriliş Şekli

Bu şartnameye uygun olarak düzenlenecek teklifler, **kapalı zarf** yolu ile İTKİB'e iletilecektir.

IV. Tekliflerin Veriliş Zamanı ve Yeri

Hazırlanan teklifler en geç **16/11/2018 saat 17:00'ye kadar** **İTKİB**'e (Çobançeşme Mevkii, Sanayi Cad. Dış Ticaret Kompleksi B Blok 3. Kat P.K.34196 Yenibosna / Bahçelievler / İSTANBUL) Satın Alma ve Destek Hizmetleri Şubesi'nden Sn. Müge Kunt Akaner'e elden veya posta yoluyla ulaştırılacaktır. Bu tarihe kadar teslim edilmeyen teklifler değerlendirmeye alınmayacaktır.

V. Teklif Öncesi Bilgilenme

YÜKLENİCİLER; şartname konusu iş ile ilgili sorularını yazılı veya sözlü olarak aşağıda belirtilen kişilere iletebileceklerdir.

İdari konular için : Müge Kunt Akaner 0212 4540217 muge.kunt@itkib.org.tr
Teknik konular için : Tayfun Yetkin 0212 4540336 tayfun.yetkin@itkib.org.tr

VI. Teklifler Hazırlanırken dikkate alınacak hususlar

YÜKLENİCİler tekliflerini hazırlarken aşağıda belirtilen hususları gözönünde bulundurmalıdır.

1. Fiyata KDV ayrıca ilave edilecektir.
2. Sözleşmeden itibaren 5 gün içerisinde **İTKİB** ile iş programı kesinleştirilecektir.
3. Sözleşmeden doğan her türlü vergi **YÜKLENİCİ**'ye ait olacaktır.
4. **YÜKLENİCİ** işi bir başkasına devredemeyecektir.

VII. Tekliflerin Geçerlilik Süresi

Teklifler veriliş tarihinden itibaren 30 gün süre ile geçerli olacaktır.

VIII. Sözleşmenin İmzalanması

İTKİB ile ihalenin üzerinde kaldığı **YÜKLENİCİ** arasında anlaşılan bedel üzerinden sözleşme imzalanacaktır.

IX. Diğer Hususlar

1. Teklifler **İTKİB** tarafından incelenip değerlendirilecek, gerekli görüldüğü takdirde teklif veren firmalar görüşme için ayrı ayrı **İTKİB**'e davet edilebilecektir.
2. Tekliflerin değerlendirme sonuçları teklif veren firmalara bildirilecektir.
3. **İTKİB** dilediği taktirde tüm alımı veya bir kısmını iptal etmekte serbesttir.
4. Firma, işbu şartname ve eklerinden doğmuş ve doğacak sorumluluklarını, hak ve alacaklarını başkalarına **İTKİB**'in yazılı onayı olmadan kısmen veya tamamen devir ve temlik edemez.
5. Bu alım ile ilgili çıkabilecek anlaşmazlıkların çözümünde İstanbul Tahkim Merkezi yetkilidir.