T.C.
TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ REKTÖRLÜĞÜ
İdari ve Mali İşler Daire Başkanlığı

Sayı :20421142-934.99/
Konu :Hizmet Alımı

Bilişim Firmaları
Yaklaşık Maliyet Araştırması

Üniversitemiz tüm birimlerinde kullanılmak üzere alımı planlanan "Bilişim Altyapısı Bilgi Güvenliği Yönetim Sistemi Danışmanlık Hizmet Alımı İşi" ve "Bilişim Altyapısı Bilgi Güvenliği Yönetim Sistemi Belgelendirme Denetim İşi" yaklaşık maliyetlerinin hesaplanabilmesi için K.D.V. hariç birim fiyatlarının karşılarına yazılarak 24/10/2018 tarihi saat 17:00'a kadar idareye elden, fax veya e-mail yoluyla bildirilmesini rica ederim.

Fatih ALHAN
Genel Sekreter

İHTİYAÇ LİSTESİ

S.NO	Malzemenin Cinsi	Birimi	Birim Fiyat	Yaklaşık Maliyet
1	Bilişim Altyapısı Bilgi Güvenliği Yönetim Sistemi Danışmanlık Hizmet Alımı	1 adet		
2	Bilişim Altyapısı Bilgi Güvenliği Yönetim Sistemi Belgelendirme Denetim Hizmet Alımı	1 adet		
			KDV HARİÇ TOPLAM	

EKLER :
1- İhtiyaç Listesi
2- Teknik Şartname

Taşlıçiftlik Yerleşkesi 60150 Tokat/Türkiye

Tel: (0356)252 15 80
Faks: (0356)252 16 05-252 16 20-252...

E-Posta: idarimali@gop.edu.tr
Elektronik ağ: idari.gop.edu.tr

Bilgi için: Ö.BAŞAR Şef
Kep Adresleri :
gaziosmanpasa.universitesi@hs03.kep.tr
gou@hs01.kep.tr (tebligat adresi)
gaziosmanpasauni.hastane@hs03.kep.tr

22/10/2018 Şef : Ö.BAŞAR
__/__/____ D.Bşk. : R.DAYAN

Taşlıçiftlik Yerleşkesi 60150 Tokat/Türkiye
Tel: (0356)252 15 80 Faks: (0356)252 16 05-252 16 20-252...
E-Posta: idarimali@gop.edu.tr Elektronik ağ: idari.gop.edu.tr
Ayrıntılı bilgi için irtibat: Ö.BAŞAR Şef

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

BİLİŞİM ALTYAPISI BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

BELGELENDİRME DENETİM İŞİ

TEKNİK ŞARTNAME

EKİM 2018

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI BİLİŞİM ALTYAPISI BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ BELGELENDİRME DENETİM İŞİ TEKNİK ŞARTNAMESİ

1.1 İŞİN TANIMI

Bu şartname Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı Bilişim Altyapısı Bilgi Güvenliği Yönetim Sisteminin TS-ISO/IEC 27001:2013 sertifikası ile belgelendirme denetimi için teknik gereksinimleri kapsamaktadır.

1.2 TANIMLAR

BGYS : TS-ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi
İdare : Tokat Gaziosmanpaşa Üniversitesi
Yüklenici : İdare tarafından kabul edilen firma

2. BELGE KAPSAMI

Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı ve ayrı kampüste bulunan Tıp Fakültesi Bilişim Altyapısına ilişkin iş süreçleri, çalışanlar ve ilgili birimleri kapsamaktadır. Denetim faaliyetinin Taşlıçiftlik Yerleşkesi ve Tıp Fakültesi Kampüsünü kapsayacak şekilde örnekleme usulü ile yapılması öngörülmekte olup, denetimci örnekleme yapılacak lokasyonu değiştirebilecektir.

3. BELGELENDİRME DENETİM HİZMETİ

3.1. Belgelendirme Denetim hizmeti sözleşme süresince bir (1) kez yapılacaktır.

3.2. Belgelendirme Denetimine, sözleşme imzalanmasından itibaren en geç onbeş (15) gün içerisinde başlanacaktır.

3.3. Belgelendirme Denetimi yapacak olan Denetçi ve Denetçilerin tüm ulaşım (gidiş/dönüş), konaklama ve iaşe giderleri yükleniciye ait olacaktır.

3.4. İdare, Belgelendirme Denetimi yapacak olan Denetçiyi değiştirme hakkına sahip olacaktır.

3.5. Yüklenici tarafından ayrıca Belge ve Logo kullanım bedeli istenmeyecektir.

3.6. Belgeler A3 ve A4 formatında, İngilizce ve Türkçe olamak üzere iki dilde hazırlanacaktır.

3.7. Yüklenici, sertifikayı Belgelendirme Denetiminden dört (4) hafta içerisinde İdareye sunacaktır.

3.8. Yüklenici, Belgelendirme Denetimi sonrası serfifikayı iptal etmesine yol açacak koşulları idareye sunacaktır.

3.9. Yüklenici belgelendirme sonrası, üç (3) adet 100x150cm ebatlarında gönder bayrağı temin edecektir.

4. BELGELENDİRME KURULUŞU

4.1. Belgelendirme kuruluşunun TS-ISO/IEC 27001:2013 TÜRKAK aktif akreditasyonu olacaktır.

4.2. TS-ISO/IEC 27001 üzerine en az üç (3) yıl süre ile denetim faaliyetleri yürütmüş ve en az bir (1) adet Kamu Kuruluşunu belgelendirmiş olacaktır.

4.3. Belgelendirme kuruluşunda en az 2 (iki) adet TS-ISO/IEC 27001:2013 akreditasyonuna sahip denetçi olmalıdır.

4.4. İşin süresi 210(ikiyüzon) takvim günüdür.

Mustafa KAPLAN
Mühendis

Şakire YÜCE
Tekniker

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI
BİLİŞİM ALTYAPISI
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ
DANIŞMANLIK HİZMET ALIMI İŞİ

TEKNİK ŞARTNAME

EKİM 2018

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI BİLİŞİM ALTYAPISI BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ **DANIŞMANLIK HİZMET ALIMI TEKNİK ŞARTNAMESİ**

1.1 İŞİN TANIMI

Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı Bilişim Altyapısı bünyesinde TS-ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi konusunda işleyen bir sistem kurmaktır. Üniversite'nin bilgi varlıklarını içeriden ve dışarıdan gelebilecek her türlü risklere ve tehditlere karşı korumaktır. Tüm çalışanlarda Bilgi Güvenliği bilinci ve farkındalığının oluşmasını sağlamak, akreditasyonlu bir ISO 27001:2013 Sertifikası ile de bu sistemin tescillenmesini sağlamak amacıyla Eğitim ve Danışmanlık Hizmeti almaktır.

1.2 TANIMLAR

BGYS : TS-ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi
İdare : Tokat Gaziosmanpaşa Üniversitesi
Yüklenici : İdare tarafından kabul edilen firma

1.3. İŞİN KAPSAMI : Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı ve ayrı kampüste bulunan Tıp Fakültesi Bilişim Altyapısına ilişkin iş süreçleri, çalışanlar ve ilgili birimleri kapsamaktadır.

2. BELGELENDİRME DANIŞMANLIK HİZMETİ

2.1. İş kapsamında, BGYS fark analizi ve kurulumu işlemleri yapılacaktır.

2.2. Proje Ekibi, Bilgi Güvenliği ve ISO 27001 eğitimleri kapsamında gerçekleştirilecek faaliyetleri yürütecektir.

2.3. Proje ekibinde, eğitmen ve/veya tahsis ettiği diğer personel haricinde, sözleşme süresince 1 (bir) Proje Yöneticisi, en az 1 (bir) Bilgi Güvenliği Uzmanı ve Eğitimci olmak üzere Bilgi Güvenliği ve ISO27001 Çalışmaları Ekibi oluşturacaktır.

2.4. Proje Yöneticisi, en az 2 (iki) yıllık iş tecrübesine sahip olmalıdır.

2.5. Bilgi Güvenliği Uzmanı, en az 2 (iki) yıllık iş tecrübesine sahip, BGYS'nin işletilmesinden sorumlu olacaktır. ISO27001 Baş Tetkikçi (Lead Auditor) sertifikasına ve EC- Council tarafından verilen CEH (Certified Ethical Hacker) sertifikalarından herhangi birine sahip olmalıdır.

3. BİLGİ GÜVENLİĞİ FARK ANALİZİ

3.1. İdarenin bilişim altyapısının ve BGYS kapsamındaki ilgili birimlerinin mevcut durumu analiz edilecek ve BGYS uyumluluğu farkı tespit edilecektir. Bu kapsamda, Yüklenicinin yapması beklenen işler aşağıda belirtilmiştir.

3.1.1. Eğitim boyunca idarenin bilişim altyapısının ve iş süreçlerinin tespiti yapılacaktır.

3.1.2. Eğitim boyunca tespit edilen altyapının ve süreçlerin BGYS ile uyumluluğu analiz edilecektir.

3.1.3. Eğitim boyunca analiz esnasında en az ISO27001:2013 BGYS standardı ve ISO27002 Bilgi Teknolojisi- Güvenlik Teknikleri- Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri kılavuzu referans alınacaktır.
3.1.4. Eğitim boyunca bunlara ek olarak ihtiyaç duyulması halinde, İdarenin de onayı alınarak İdareye özel ek kontrol maddeleri eklenebilecektir.
3.1.5. Eğitim boyunca her bir kontrol maddesi için en az aşağıdakileri içerecek şekilde analiz yapılacaktır.
3.1.5.1 Kontrol maddesi numarası verilecektir.
3.1.5.2 Standart maddesinin tanımı yapılacaktır.
3.1.5.3 Standart maddesinin açıklaması yapılacaktır.
3.1.5.4 İdarede uygulanan mevcut durum açıklanacaktır.
3.1.5.5 Standart ile mevcut durum arasındaki farklar raporlanacaktır.
3.1.6 Eğitim boyunca yapılan analiz sonucunda Mevcut Durum Analiz Raporu oluşturulacaktır. Oluşturulacak rapor, yönetici özeti, analiz edilen sistemler, fark analizi, tespit edilen saldırı ve tehditler, sistem işleyişi ile ilgili gözlemlenen sorunlar, çözüm ve iyileştirme önerileri ve sonuç bölümlerinden oluşacaktır.
3.1.7 Eğitim boyunca oluşturulacak rapor 20 (yirmi) iş günü içerisinde bir toplantı ile İdareye sunulacaktır.
3.1.8. Eğitim boyunca oluşturulan raporun sonucuna göre BGYS proje planı oluşturulacaktır.
3.1.9. Eğitim boyunca proje planı İdare tarafından değerlendirilecek ve en geç 5 (beş) iş günü içerisinde Yükleniciye geri bildirim verilecektir.
3.1.10. Yüklenici, proje planını İdarenin istediği şekilde en geç 10 (on) iş günü içerisinde düzenleyecek ve tekrar İdarenin onayına sunacaktır. Proje planının onaylanmasından sonra çalışmalara başlanacaktır.

4. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) KURULUMU İŞLEMLERİ

Süreç boyunca bilgi güvenliği fark analizi başlığı altında tespit edilen uygunsuzluklar ile ilgili çalışmalar yapılarak, ISO27001:2013 BGYS Standardına uygun bir BGYS'nin kurulması sağlanacaktır. Bu kapsamda, Yüklenicinin yapması beklenen işler aşağıda belirtilmiştir.

4.1. Fark analizi sonuçlarına göre İdare yapısına uygun ve en az ISO27003 Bilgi teknolojisi-Güvenlik Teknikleri- BGYS Uygulama Kılavuzunda belirtilen hususları karşılayacak şekilde bir BGYS organizasyonu oluşturulacaktır.
4.2. Fark analizi sonuçlarını, Eğitim planını, organizasyon yapısını ve üst yönetici bilgi güvenliği farkındalık konularını içeren, üst yönetimin proje desteğinin alınmasını sağlamak amacıyla üst yönetim sunumu yapılacaktır.
4.3. BGYS Eğitimi başlaması için gerekli olan, en az aşağıda belirtilen temel dokümanlar hazırlanacaktır.
4.3.1 Doküman Yönetimi Prosedürü hazırlanacaktır.
4.3.2 Kapsam analizi dokümanı hazırlanacaktır.
4.3.3 Kapsam analizi dokümanı oluşturulurken en az aşağıdaki başlıklarda analiz yapılacaktır.
4.3.3.1 İdarenin stratejisi, amaçları ve hedefleri belirlenecektir.
4.3.3.2 İdarenin iç hususları ve BGYS hedeflerine etkisi belirlenecektir.
4.3.3.3 İdarenin dış hususları ve BGYS hedeflerine etkisi belirlenecektir.
4.3.3.4 İdarenin yasal yükümlülükleri ve BGYS hedeflerine etkisi belirlenecektir.
4.3.3.5 İdarenin kritik varlıkları ve süreçleri belirlenecektir.

4.3.3.6 İlgili tarafların İdareden bilgi güvenliği beklentileri belirlenecektir.
4.3.3.7 Bilgi güvenliği politikası belirlenecektir.
4.3.3.8 Varlık yönetimi prosedürü belirlenecektir.
4.3.3.9 Risk yönetimi prosedürü belirlenecektir.
4.3.3.10 Roller ve sorumluluklar dokümanı
4.4. Oluşturulan temel dokümanlar İdarenin onayına sunulacaktır ve eğitimi tamamlanacaktır.
4.5. Bilgi Varlık envanteri tespiti yapılacaktır.

4.5.1 Varlık envanteri tespiti ilgili birimler ile yapılacak birebir görüşmeler ile gerçekleştirilecektir.

4.5.2. Oluşturulan varlık envanteri en az aşağıdaki bilgileri içerecek şekilde, elektronik ortamda İdarenin onayına sunulacaktır.Varlık adı, Varlık açıklaması, Varlık sahibi, Varlığın konumu, Varlığın miktarı, Gizlilik, bütünlük ve erişilebilirlik değerleri, Varlığa ilişkin tanımlayıcı diğer teknik özellikler (IP adresi, host name vb.)
4.5.3. Teknik risk analizi ile ilgili detaylar Teknik Açıklık Testleri başlığı altında detaylandırılacaktır. Kavramsal risk analizi yapılırken en az aşağıdaki hususlar dikkate alınacaktır.

4.5.3.1. Kavramsal risk analizi İdarenin ilgili birimleri ile yapılacak birebir görüşmeler ile yapılacak sonra eğitime geçilecektir.

4.5.3.2. Fark analizi sonuçları dikkate alınacaktır.

4.5.3.3.Varlığın/sürecin gizliliğini, bütünlüğünü veya erişilebilirliğini tehdit eden unsurlar ve bu tehdide neden olacak zafiyetler tespit edilecektir ve buna göre kavramsal risk analizi yapılacaktır.
4.5.3.4. Kavramsal risk analizi eğitimi en az aşağıdaki tehdit ve zafiyet alanlarını içerecek şekilde yapılacaktır.
4.5.3.5.Dış kurum, kişiler ve paydaşlardan gelecek tehditler
4.5.3.6.Bilişim sistem operasyonları ve işletmesinden kaynaklanacak tehditler
4.5.3.7.Bilişim eleman ve kullanıcılarından gelecek tehditler
4.5.3.8.Organizasyon ve iş sorumluluklarından gelecek tehditler
4.5.3.9.Yazılım geliştirme ortamlarından gelebilecek tehditler
4.5.3.10. Bilişim ağ ve sunucu sistem yönetim işlevlerinden gelebilecek tehditler
4.5.3.11. Fiziksel ve mantıksal erişim tehditleri
4.5.3.12. Doğal koşul ve felaketlerden gelecek tehditler
4.6. Eğitim kapsamında riskin varlık veya süreç üzerindeki etkisi ve oluşma olasılığına göre risk puanı hesaplanacaktır.
4.7. Risk puanına göre alınması gereken risk işleme kararı belirlenecektir.
4.8. Tespit edilen riskler ve risk işleme kararları İdare proje ekibi ile birlikte değerlendirilecektir.
4.9. Risk analizi sonucunda tehdit ve zafiyetleri içeren bir risk listesi oluşturulacaktır. Oluşturulacak listede en az aşağıdaki bilgiler yer alacaktır.

4.9.1. Etkilenen varlık/süreç belirlenecektir.

4.9.2. Varlığın/sürecin Sonuç Değeri belirlenecektir.

4.9.3. Tehdit tanımı yapılacaktır.

4.9.4. Zafiyet tanımı belirlenecektir.

4.9.5. Tehdidin Oluşma Olasılığı belirlenecektir.

4.9.6. Tehdidin etki Derecesi belirlenecektir.

4.9.7. İlk Risk değeri belirlenecektir.

4.9.8. Risk işleme faaliyetleri belirlenecektir.

4.9.9. Faaliyetler Sonrası Tehdidin Oluşma Olasılığı belirlenecektir.

4.9.10. Faaliyetler Sonrası Tehdidin Etki Derecesi belirlenecektir.

4.9.11. Son Risk Değeri belirlenecektir.

4.10. Eğitim kapsamında risk işleme planından sonra Uygulanabilirlik Bildirgesi hazırlanacaktır. Bildirgede en az aşağıdaki bilgiler yer alacaktır.

4.10.1. TS ISO/IEC 27001:2013 Kontrol konusu belirlenecektir.

4.10.2. TS ISO/IEC 27001:2013 Kontrol maddeleri belirlenecektir.

4.10.3. Kontrol maddesinin uygulanıp uygulanmadığı belirlenecektir.

4.10.4. Referans dokümanı hazırlanacaktır.

4.11. Eğitim kapsamında uygulanabilirlik bildirgesinde belirtilen referans dokümanları Yüklenici tarafından oluşturulacaktır.

4.12. Oluşturulacak dokümanlar İdarenin iş hedeflerine ve mevzuata uyumlu olacaktır.

4.13. Oluşturulacak dokümanlar Hedef kullanıcı ve sorumluları tarafından anlaşılır nitelikte olacaktır.

4.14. Eğitim kapsamında en az aşağıdaki alanlarda dokümanlar oluşturulacaktır. Dokümanlar İdare tarafından onaylanan Doküman Yönetimi Prosedürüne uygun şekilde oluşturulacaktır.

5. BGYS Prosedürleri

5.1. İş Sürekliliği Prosedürü hazırlanacaktır.

5.2. Değişiklik Yönetim Prosedürü hazırlanacaktır.

5.3. Internet Erişim Prosedürü hazırlanacaktır.

5.4. Yedekleme Prosedürü hazırlanacaktır.

5.5. Görevler Ayrılığı Prosedürü hazırlanacaktır.

5.6. İç Tetkik Prosedürü hazırlanacaktır.

5.7. Yönetimin Gözden Geçirmesi Prosedürü hazırlanacaktır.

5.8. Yasal Gereksinimlere Uyum Prosedürü hazırlanacaktır.

5.9. Bilgi Güvenliği İhlal olayı yönetimi prosedürü hazırlanacaktır.

5.10. Teknik açıklık prosedürü hazırlanacaktır.

5.11. Teçhizat güvenliği prosedürü hazırlanacaktır.

5.12. Fiziksel güvenlik prosedürü hazırlanacaktır.

5.13. Düzeltici ve İyileştirici Faaliyet Prosedürü hazırlanacaktır.

5.14. İnsan Kaynakları Güvenliği Prosedürü, personel planlama ve personel sorumlulukları dokümanı hazırlanacaktır.

5.15. Personel İlişik Kesme Esasları hazırlanacaktır.

5.16. Ağ güvenliği yönetimi prosedürü hazırlanacaktır.

5.17. Kullanıcı Eğitim Dokümanı hazırlanacaktır.

6. BGYS Politikaları

Yüklenici aşağıdaki politikaları hazırlayacaktır.

6.1. Bilgi Güvenliği Politikası hazırlanacaktır.

6.2. Parola Politikası hazırlanacaktır.

6.3. Temiz Masa ve Temiz Ekran Politikası hazırlanacaktır.

6.4. Uzaktan Erişim ve Çalışma Politikası hazırlanacaktır.

6.5. Mobil Cihaz/Dizüstü Bilgisayar Kullanımı Politikası hazırlanacaktır.

6.6. Varlıkların Kabul edilebilir Kullanımı Politikası hazırlanacaktır.

6.7. Tedarikçi İlişkileri Yönetimi Politikası hazırlanacaktır.

6.8. Erişim Kontrol Politikası hazırlanacaktır.

6.9. Siber Saldırılara Karşı Korunma Alt Politikası hazırlanacaktır.

6.10. Basılı Çıktı Güvenlik Politikası hazırlanacaktır.

6.11. Gizlilik Anlaşması Dokümanı hazırlanacaktır.

6.12. Dış bağlantı Güvenliği Esasları hazırlanacaktır.

7. Talimatlar

Yüklenici aşağıdaki talimatları hazırlayacaktır.

7.1. Yedekleme Talimatı hazırlanacaktır.

7.2. Veri tabanı Kullanım ve Kurulum Talimatı hazırlanacaktır.

7.3. Güvenlik Duvarı Kullanım Talimatı hazırlanacaktır.

7.4. Sistem Odası Kullanım Talimatı hazırlanacaktır.

7.5. Antivirüs Yapılandırma Talimatı hazırlanacaktır.

7.6. Ağ Alt Yapısı Standartları hazırlanacaktır.

7.7. Kullanıcı kimliği ve e-posta tanımlama esasları hazırlanacaktır.

7.8. İşletim Sistemleri Güvenlik Kuralları hazırlanacaktır.

7.9. İnternet Erişim Kuralları hazırlanacaktır.

7.10. Kullanıcı Bilgilendirme Kuralları hazırlanacaktır.

7.11. Yedekten Geri Dönüş Esasları hazırlanacaktır.

7.12. Bilgisayar Elden Çıkarma Esasları hazırlanacaktır.

7.13. Veri Tabanı Yedekleme ve Bakım Esasları hazırlanacaktır.

7.14. Yazılım Kurulumu Esasları hazırlanacaktır.

7.15. Kullanıcı Bilgisayarları Kurulum ve Kullanım Esasları hazırlanacaktır.

7.16. Bunlara ek olarak İdare'nin ihtiyaç duyduğu talimatlar Yüklenici tarafından oluşturulacaktır.

8. Form ve Listeler

Yüklenici aşağıdaki form ve listeleri hazırlayacaktır.

8.1. Güvenlik Olay Bildirim Formu hazırlanacaktır.

8.2. Güvenlik Olay Raporlama Formu hazırlanacaktır.

8.3. Değişiklik Talep Formu hazırlanacaktır.

8.4. Teçhizatın elden çıkartılması formu hazırlanacaktır.

8.5. Yedekten dönüş formu hazırlanacaktır.

8.6. Teçhizat dışarı çıkarma formu hazırlanacaktır.

8.7. Proje yönetimi formu hazırlanacaktır.

8.8. Düzeltici ve İyileştirici Faaliyet formu hazırlanacaktır.

8.9. Ayrıcalıklı kullanıcı yetki talep ve yetkilendirme formu hazırlanacaktır.

8.10. BT istek formu hazırlanacaktır.

8.11. İç tetkik planı hazırlanacaktır.

8.12. İç tetkik rapor formu hazırlanacaktır.

8.13. Eğitim katılımcı imza listesi hazırlanacaktır.

8.14. Toplantı tutanağı hazırlanacaktır.

9. Diğer Hükümler

9.1. Oluşturulacak dokümanlar İdare tarafından kontrol edilecek ve değişiklik talepleri Yükleniciye bildirilecektir. Yüklenici her bir doküman için bildirim tarihinden sonra en geç 3 (üç) iş günü içerisinde revize dokümanı İdare ile paylaşacaktır.
9.2. Dokümanların son hali İdare tarafından onaylanacaktır.
9.3. Dokümanların ilgili kullanıcılara duyurulması ve yaygınlaştırılması İdarenin sorumluluğundadır.
9.4. Risk işleme faaliyetleri tamamlandıktan sonra yüklenici tarafından İdare personelinin de katılımıyla iç tetkik eğitimi ile birlikte gerçekleştirilecektir. İç tetkikler aşağıdaki hususlar göz önüne alınarak yapılacaktır.
9.4.1. İç tetkik planı prosedürde belirtildiği şekilde oluşturulacak ve İdare ile paylaşılacaktır.
9.4.2. İç tetkik, proje içerisinde yer almamış ve ISO27001:2013 Baş Denetçi sertifikasına sahip denetçi tarafından gerçekleştirilecektir.
9.4.3. İç tetkik raporu tetkikin tamamlanmasından en geç 5 (beş) iş günü içerisinde teslim edilecektir.
9.4.4. İç tetkikte tespit edilen bulguların giderilmesi için İdareye yol göstericilik yapılacaktır.
9.5. 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.
9.6. İşin süresi 120(yüzyirmi) takvim günüdür.

Mustafa KAPLAN
Mühendis

Şakire YÜCE
Tekniker