

ISO 27001:2022 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VERSİYON GEÇİŞ EĞİTİMİ VE DANIŞMANLIK HİZMET ALIMI TEKNİK ŞARTNAMESİ

1. Şartnamenin Konusu

1.1. Türkiye Şeker Fabrikaları A.Ş. Merkez Teşkilatında bulunan ilgili Daire Başkanlıklarında görev yapan personele; ISO 27001:2022 Temel Eğitimi, ISO 27001:2022 Versiyon Geçiş Eğitimi, ISO 27001:2022 Dokümantasyon Eğitimi ve ISO 27001:2022 İç Tetkik Eğitimi verilmesi; eğitim sonunda katılımcıların ölçme-değerlendirme ile sınanması ve sertifikalandırılması işidir.

1.2. Merkez Teşkilatının mevcut ISO 27001 BGYS dokümanlarının ISO 27001:2022'ye uyumlu hale getirilmesi; ek dokümanların hazırlanmasına teknik danışmanlık verilmesi; gözetim/yenileme denetimleri ve belgelendirme sürecinde kanıt yönetimi, denetim hazırlığı ve denetime eşlik desteği verilmesi işidir.

2. Tanımlar ve İdareye İlişkin Bilgiler

İş Sahibi İdareye İlişkin Bilgiler

Adı : Türkiye Şeker Fabrikaları A.Ş. Genel Müdürlüğü

Adresi : Mithatpaşa Cad. No:14 Yenışehir/ANKARA

Bu teknik şartnamede geçen;

- İdare: Türkiye Şeker Fabrikaları A.Ş. Genel Müdürlüğünü,
- Merkez Teşkilatı: Genel Müdürlüğü,
- Başkanlık: Bilgi Teknolojileri Daire Başkanlığını,
- Yüklenici: Bu şartname kapsamında sözleşme imzalanan istekliyi,
- Yüklenici Personeli: Şartnamede tanımlanan eğitim ve danışmanlık faaliyetlerini yürütecek yüklenici personelini ifade eder.


3. İşin Yapılma Şartları, Kapsam ve Teslimatlar

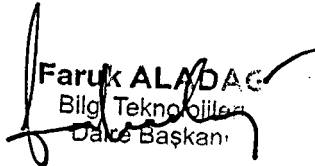
3.1. Eğitimler, Kalite Yönetim Sistemi Ekibi ve Merkez Teşkilatına bağlı ilgili Daire Başkanlıklarında görev yapan personele Genel Müdürlük yerleşkesinde verilecektir. Eğitimleri müteakip, Merkez Teşkilatında mevcut BGYS dokümanlarının ISO 27001:2022'ye uyumlandırılması ve ilave dokümanların hazırlanması kapsamında danışmanlık hizmeti verilecektir.

3.2. Eğitimler her başkanlıktan 2'şer kişi ve Bilgi Teknolojileri Daire Başkanlığı personeli olacak şekilde planlanacaktır (yaklaşık 50 personel). Eğitimler aşağıdaki konuları kapsayacaktır:

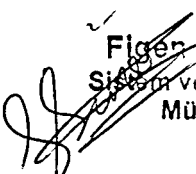
- ISO 27001:2022 BGYS Temel Eğitimi
- ISO 27001:2022 BGYS Versiyon Geçiş (2017/önceki sürümden 2022'ye farklar) Eğitimi
- ISO 27001:2022 BGYS Dokümantasyon ve Kanıt Yönetimi Eğitimi
- ISO 27001:2022 BGYS İç Tetkik Eğitimi (uygulamalı)

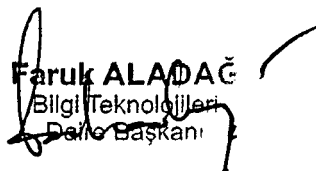
3.3. Mevcut dokümanların ISO 27001:2022'ye adaptasyonu ve gerekli ilave dokümanların hazırlanması, Merkez Teşkilatında yürütülecek; her başkanlık için ihtiyaç duyulan dokümanlar tamamlanacaktır.


Figen SÜZER
Sistem ve Güvenlik
Müdürü


Faruk ALADAĞ
Bilgi Teknolojileri
Daire Başkanı

- 3.4.** Yüklenici; eğitim programını, eğitmen listesini ve görevlendirilecek personelin eğitimleri vereceğine dair yazılı ve imzalı beyanı teklif ekinde sunacaktır. Program; eğitim başlıkları, süreler, içerik kırılımı, uygulama/atölye süreleri ve ölçme-değerlendirme yaklaşımını içerecektir.
- 3.5.** Eğitim günlerinde eğitimler 08.30-17.30 saatleri arasında, 12.15-13.30 öğle dinlenme arası hariç tutulacak şekilde planlanacaktır. Elzem durumlarda eğitim saatlerinde değişiklik yapma yetkisi, önceden bildirilmek suretiyle Başkanlığa aittir.
- 3.6.** Eğitimler, Başkanlık tarafından görevlendirilecek eğitim koordinatörü ve/veya program yöneticisi organizasyonunda verilecektir. Yüklenici, Başkanlık ile mutabakat sağladıktan sonra eğitim programında gerekli gördüğü değişiklikleri yapabilecektir.
- 3.7.** Yüklenici, teklif ettiği personeli İdarenin onayı olmadan değiştiremez. Zorunlu hallerde personel değişikliği; eğitim/danışmanlık tarihinden önce Başkanlığın yazılı onayı alınarak ve yerine atanacak personelin nitelikleri bu şartnamede belirtilen minimum şartları sağlayacak şekilde yapılacaktır.
- 3.8.** Yüklenici; ders notu, kitap, şablon doküman, kontrol listeleri vb. dokümanları teklifinde açıkça belirtecektir. Her eğitim için yazılı ve dijital ortamda hazırlanacak ders notu eğitimden önce Başkanlığa teslim edilecektir. Ders notları; eğitim süresi, konu kapsamı ve ISO 27001:2022'nin gerektirdiği uygulama örnekleri ile uyumlu olacaktır. Doküman çoğaltımı yüklenici sorumluluğundadır.
- 3.9.** Eğitim esnasında ihtiyaç duyulacak projeksiyon cihazı, bilgisayar vb. araç-gereç temini İdarenin sorumluluğundadır.
- 3.10.** Başkanlık, Yükleniciye en az 10 (on) gün önceden bildirmek suretiyle eğitimin yapılmasından vazgeçebilir veya eğitimin tarihinde değişiklik yapabilir.
- 3.11.** Eğitimlerin asgari süreleri aşağıdaki gibidir (İdarenin ihtiyacına göre süre artırılabilir):
- Temel Eğitim: en az 12 saat (2 gün)
 - Versiyon Geçiş Eğitimi: en az 6 saat (1 gün)
 - Dokümantasyon ve Kanıt Yönetimi Eğitimi: en az 6 saat (1 gün)
 - İç Tetkik Eğitimi: en az 12 saat (2 gün) ve en az 1 uygulamalı tetkik senaryosu çalışması
- 3.12.** Eğitim sonunda, asgari 30 (otuz) sorudan oluşan, test usulü, 4 (dört) seçenekli ölçme-değerlendirme sınavı yapılacaktır. Sınav soruları; en az %30 bilgi, %40 senaryo/yorum ve %30 uygulama odaklı olacak şekilde dağılımlı hazırlanacaktır. Sorular, cevap anahtarları ve sınav sonuçları Başkanlığa teslim edilecektir. Soruların ve cevap anahtarlarının gizliliği esastır.
- 3.13.** Eğitim sonunda yüklenici tarafından her katılımcıya sınavdaki başarısına göre 'Başarı Belgesi' düzenlenerek Başkanlığa teslim edilecektir. Başarı puanı 100 tam puan üzerinden en az 60 tam puandır. (Başarısız katılımcılar için bir (1) kez ücretsiz telafi sınavı yapılacaktır.)
- 3.14.** Yüklenici personeli, eğitim sonunda genel değerlendirme yaparak; uygulama hakkındaki görüşleri ve önerileri içeren bir değerlendirme raporunu Başkanlığa sunacaktır.
- 3.15.** Yüklenici, Merkez Teşkilatında sistemin (BGYS'nin) ISO 27001:2022'ye adaptasyonu ile ilgili gerekli inceleme ve araştırmaları yapacak; BGYS ve uygulanmasına yönelik olarak karşılaşılabilecek sorunlara şartname ve sözleşme ruhuna uygun çözümler önerecek; gerektiğinde üçüncü taraflarla (belgelendirme kuruluşu vb.) koordinasyona destek olacaktır.
- 3.16.** Merkez Teşkilatında mevcut ISO 27001 BGYS'nin ISO 27001:2022'ye adaptasyonu yapılacak; uygulanabilirliği sağlanarak belgelendirme aşamasına getirilecektir.


Figen SÜZER
Sistem ve Güvenlik
Müdürü


Faruk ALADAĞ
Bilgi Teknolojileri
Daire Başkanı

3.17. Zorunlu Teslimatlar: Yüklenici, danışmanlık kapsamında aşağıdaki doküman ve çıktıları idareye teslim edecektir:

- ISO 27001:2022 Geçiş (Transition) GAP Analizi Raporu (bulgu-aksiyon-sorumlu-tarih içerecek şekilde)
- Geçiş Proje Planı ve haftalık durum/aksiyon kayıtları (risk-issue-action log)
- Güncellenmiş Uygulanabilirlik Bildirimi (SoA) ve kontrol-gerekçe/kanıt referansları
- Güncellenmiş risk değerlendirme metodolojisi, risk kayıtları ve risk işleme planı
- Annex A 2022 Kontrol-Kanıt Matrisi (kontrol -> kanıt türü -> kanıt sahibi -> kanıt lokasyonu -> güncellik)
- İç tetkik programı, kontrol listeleri, örnek tetkik senaryosu ve en az 1 prova (mock audit) raporu
- Yönetimin gözden geçirmesi gündemi, şablonları ve ilk toplantı çıktısı (karar/aksiyonlar)
- Belgelendirme hazırlık paketi (Stage 1/Stage 2 için kanıt listesi ve izlenebilirlik matrisi)

3.18. Dokümanların Formatı ve Revizyon: Teslim edilecek tüm dokümanlar MS Word formatında, revizyon tablosu ve doküman numaralandırması içerecek; İdarenin mevcut doküman şablonlarına uyumlu biçimde hazırlanacaktır.

3.19. Kabul ve Revizyon Döngüsü: İdare, her teslimatı en geç 5 (beş) iş günü içinde inceleyip geri bildirim verecektir. Yüklenici, geri bildirimleri en geç 5 (beş) iş günü içinde revize ederek yeniden sunacaktır. Kabul, Başkanlığın yazılı onayı ile tamamlanır.

3.20. Çalışma Modeli ve Erişim: Yüklenici, işi yürütmek için asgari toplam 12 (on iki) iş günü yerinde (onsite) çalışmayı ve en az 6 (altı) adet çalıştay/atölye oturumu gerçekleştirmeyi taahhüt eder. Yerinde gün sayısı, İdare ihtiyacına göre artırılabilir.

3.21. Gizlilik ve Veri Koruma: Yüklenici ve personeli; kurum bilgi varlıklarının gizliliğini korumakla yükümlüdür. İdare onayı olmadan doküman ve kayıtlar bina dışına çıkarılamaz. Yüklenici, gizlilik taahhünamesini teklif ekinde sunacaktır.

3.22. Teklif fiyatı iş bu şartnamede belirtilen işin tamamını kapsayacaktır.

4. Yüklenicide Aranacak Özellikler

4.1. Yüklenici; işi yürütmek üzere asgari aşağıdaki rolleri görevlendirecektir:

- Proje Lideri / Baş Danışman (1 kişi)
- Eğitimci (en az 1 kişi, Proje Lideri ile aynı kişi olabilir)
- Dokümantasyon ve Risk Uzmanı (1 kişi, Proje Lideri ile aynı kişi olabilir)

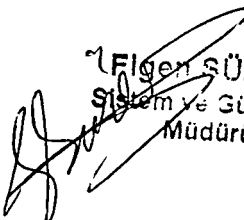
4.2. Proje Lideri / Baş Danışman için asgari şartlar:

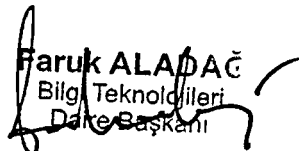
- ISO/IEC 27001 Lead Auditor (IRCA veya eşdeğeri) veya ISO/IEC 27001 Lead Implementer belgesi olmalı ve belge teklif aşamasında verilmelidir.
- En az 5 (beş) yıl BGYS kurulum/uygulama/danışmanlık/denetim deneyimi (SGK hizmet dökümü ve CV) teklif aşamasında verilecektir.

4.3. Eğitim verecek personel için asgari şartlar:

- ISO 27001:2022 eğitim/uygulama yetkinliğini gösterir sertifika veya eğitim katılım belgeleri teklif aşamasında verilecektir.
- En az 5 (beş) yıl veya 200 adam/gün BGYS eğitim deneyimi olmalı, SGK hizmet dökümü ve CV'de gösterilmelidir.

4.4. Yüklenici; teklifinde görev alacak personelin isim/unvanlarını, sertifika numaralarını (varsa doğrulama bilgileri) ve yüklenici onaylı fotoğraflı kısa özgeçmişlerini sunacaktır.


Figen SÜZER
Sistem ve Güvenlik
Müdürü


Faruk ALADAĞ
Bilgi Teknolojileri
Daire Başkanı

4.5. Yüklenici; İdarenin yazılı izni olmadan işin tamamını veya bir kısmını başka bir firmaya/şahsa devredemez. Alt yüklenici kullanımı söz konusu ise alt yüklenici bilgileri ve sorumluluk kapsamı teklif ekinde açıkça belirtilir; nihai sorumluluk yüklenicide kalır.

4.6. Yüklenici referans teslimi:

ISO 27001:2022 versiyon geçiş projesinde (2017/önceki sürümden 2022'ye) danışmanlık verilen en az 3 (üç) kurumdan referans teklif aşamasında verilecektir. Referanslardan en az 1'i (biri) kamu olmalıdır. Referanslar İdare tarafından kontrol edilecektir.

4.7. Denetim desteği: Merkez Teşkilatının 2026 yılı belge yenileme/gözetim tetkikinde Yüklenici, İdareye denetim hazırlığı ve denetimde eşlik desteği verecektir. Yüklenicinin kusurundan kaynaklanan (ör. yanlış/eksik SoA, izlenebilirlik, hatalı doküman) durumlarda, belgelendirme sürecinin tamamlanmasına kadar gerekli revizyon ve ek çalışma desteği için ayrıca ücret talep edilmeyecektir. (Belgelendirme kuruluşu ücretleri, idarenin kapsam değişikliği veya üçüncü taraflardan kaynaklanan durumlar bu madde dışındadır.)

4.8. Belge yenilenene kadar İdarenin iş ile ilgili sorularına cevap verme: Yüklenici, denetim dönemi boyunca iş kapsamında soruları cevaplayacak; kritik denetim sorularına 4 saat, diğer sorulara 1 iş günü içinde geri dönüş sağlayacaktır. Bu destek için ayrıca ücret talep edilemez.

4.9. Yüklenici, belgenin geçerlilik süresi boyunca ara denetimlerde (gözetim) destek sağlayacaktır. Destek kapsamı; denetim öncesi kanıt gözden geçirme, SoA/risk kayıtları güncellik kontrolü ve denetimde çevrimiçi/yerinde eşlik faaliyetlerini içerir.

4.10. Yüklenici, kendi personelinin bütün masraflarını (ulaşım, konaklama, yemek vb.) karşılayacaktır.

5. Performans Değerlendirmesi ve Cezai Şartlar

5.1. Yüklenici, eğitimleri programına uygun, zamanında ve katılımcıların seviyesine uygun olarak gerçekleştirmekten sorumludur. Eğitim saatlerine/konularına uyulmaması, şartnameye aykırılık, teslimat gecikmesi veya kabul kriterlerini karşılamayan teslimat olması durumlarının her biri için eğitime/danışmanlığa ait sözleşme bedelinin %10'u oranında ceza uygulanır.

5.2. Yüklenici, Başarı Belgelerini tanzim edip 10 (on) iş günü içinde İdareye teslim etmezse sözleşme bedelinin %10'u oranında ceza uygulanır.

5.3. Yüklenici, Başarı Belgelerini tanzim edip İdareye teslim etmediği takdirde ücret tahakkuku yapılmaz.

5.4. Teslimatların gecikmesi halinde; gecikilen her iş günü için sözleşme bedelinin %0,5'i oranında gecikme cezası uygulanır. Toplam gecikme cezası sözleşme bedelinin %10'unu aşamaz.

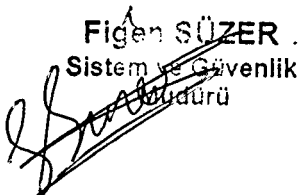
6. İşe Başlama, Süre ve Ödeme Şartları

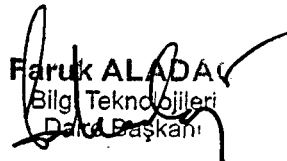
6.1. İşe başlama tarihi sözleşme imzalanmasını müteakip 7 gündür.

6.2. Sözleşme konusu eğitim ve danışmanlık hizmetinin süresi 60 (altmış) gündür. Sözleşme konusu hizmet, İdarenin ISO 27001 dış denetimi tamamlayarak yeni versiyona ait belgeyi almasıyla tamamlanmış olacaktır.

6.3. Ödeme şartları:

- Madde 1.1 ve 1.2 kapsamındaki eğitim hizmetleri verilmesi, dokümantasyon adaptasyonunun tamamlanması ve dış denetim/belgelendirme aşamasına gelinmesi durumunda sözleşme bedelinin %60'ı,
- Dış denetimin gerçekleştirilerek belgelendirme işleminin tamamlanması durumunda sözleşme bedelinin %40'ı,


Figen SÜZER .
Sistem ve Güvenlik
Bölüm Başkanı


Faruk ALADAĞ
Bilgi Teknolojileri
Bölüm Başkanı

- İşlerin tamamlanmasını müteakip Bilgi Teknolojileri Daire Başkanlığınca düzenlenecek Hizmet Kabul Tutanağı ve yüklenicinin faturalarının Satınalma Daire Başkanlığına ulaşmasından sonra, Hizmet Kabul Tutanağı tarihini izleyen 30 (otuz) gün içinde yapılacaktır.

EK-1: Asgari Doküman ve Kayıt Listesi (Örnek)

İdarenin mevcut dokümantasyon yapısına göre aşağıdaki doküman/kayıtların güncellenmesi veya oluşturulması beklenir. Nihai liste GAP analizi çıktısına göre netleştirilecektir.

- BGYS kapsam, bağlam (iç/dış hususlar) ve ilgili taraflar beklentileri dokümanı
- BGYS politikası ve ölçülebilir hedefler
- Risk değerlendirme ve risk işleme prosedürü + risk kayıtları
- SoA (Uygulanabilirlik Bildirimi) ve kontrol/kanıt referansları
- Varlık envanteri, sınıflandırma ve bilgi etiketleme yaklaşımı
- Erişim kontrol politikası, yetkilendirme matrisi, ayrıcalıklı hesap yönetimi
- Tedarikçi güvenliği prosedürü ve sözleşme güvenlik maddeleri
- Olay yönetimi prosedürü ve kayıtları
- Yedekleme/geri dönüş prosedürü ve test kayıtları
- Loglama ve izleme politikası + log kaynak matrisi
- Değişiklik ve konfigürasyon yönetimi prosedürleri
- İç tetkik programı, kontrol listeleri, bulgu/aksiyon takip kayıtları
- Yönetimin gözden geçirmesi şablonları ve toplantı çıktıları



Faruk ALADAC
Bilgi Teknolojileri
Daire Başkanı

Faruk ALADAC
Bilgi Teknolojileri
Daire Başkanı