**FİRMA ADI:**

|  |
| --- |
| **A1. İş Türleri ve Düzenleyici Gereksinimler** |
| **Kritik İş Sektörlerinden Herhangi Bir Müşteriniz Var mı? (1)**[ ]  Evet [ ]  Hayır | **Kritik İş Sektörlerinde Kurum İşleriniz Var mı? (1)**[ ]  Evet [ ]  Hayır |
| ***(1)*** *Kritik iş sektörleri, ülkeye çok büyük olumsuz etki edebilecek işlevlere, hükümet yetkilerine, imaja, ekonomiye, güvenliğe, sağlığa karşı risk oluşturabilecek kritik kamu hizmetlerini etkileyebilecek sektörlerdir.* |
| **Vermiş Olduğunuz Ürün/Hizmet Kapsamınız İle İlgili Bilgiler Aşağıdakileri İçeriyor mu?**[ ]  Evet [ ]  Hayır*Evet, ise lütfen açıklayınız.* [ ]  Maaşlar, yardımlar, sağlık ve güvenlik, kurumsal kayıtlar, birim/bölüm içi ve bölümler arası bilgiler vb.[ ]  Diğer kişisel bilgiler[ ]  Diğer ticari açıdan hassas/önemli bilgi, örneğin; araştırma ve geliştirme bilgisi, tasarım bilgileri, müşteri bilgileri, finansal tahminler ve sonuçlar, iş planları, fikri mülkiyet hakları, üretim süreçleri vb. gibi ticari olarak hassas kritik bilgiler |
| **BGYS Kapsamında Kamusal Bilgiler/Kayıtlar Yer Alıyor mu?**[ ]  Evet [ ]  Hayır*Evet, ise lütfen açıklayınız.* [ ]  Toplumsal bilgiler[ ]  E-devlet uygulamaları[ ]  Vatandaşlık bilgileri (örneğin; sağlık, yardımlar, vergiler, kayıtlar vb.)[ ]  Devletin tedarikçileri ve üreticileri tarafından işlenen, bilgi ve iletişim teknolojileri (ICT) tasarımları, tesisler, ürünler, hizmetler vb. bilgiler[ ]  Diğer (*açıklayınız*)       |
| **BGYS Kapsamında Uymakla Yükümlü Olduğunuz Yasal Şartlar ve Düzenleyici Gereksinimler (2) ile Sözleşme/İş Şartları:***Lütfen bilgi veriniz.*      |
| ***(2)*** *Düzenleyici gereksinimler kuruluşunuzun uymakla yükümlü olduğu; Bilgi Teknolojileri ve İletişim Kurumu (BTK), Enerji Piyasası Düzenleme Kurumu (EPDK), Sermaye Piyasası Kurulu (SPK), Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Kamu İhale Kurumu (KİK), Radyo ve Televizyon Üst Kurulu (RTÜK), Kişisel Verileri Koruma Kurumu (KVKK) gibi ulusal düzenleyici kurumların şartları ile uluslararası düzenleyici kurumların şartlarını içerir. Bu bölümde lütfen bu düzenleyici gereksinimlerin adlarını açıkça belirtiniz.* |
| **Düzenleyici Gereksinimleriniz Aşağıdaki Hangi Kategorileri İçermektedir? *(Lütfen işaretleyiniz)*:**  |
| [ ]  D01- Fikri Mülkiyet[ ]  D02- Kurumsal Kayıtların İçerikleri, Korunması ve Saklanması[ ]  D03- Veri Koruma ve Mahremiyet[ ]  D04- Kriptografik Kontrollerin Düzenlenmesi[ ]  D05- Elektronik Ticaret[ ]  D06- Elektronik ve Sayısal İmzalar[ ]  D07- İşyeri İzlemesi | [ ]  D08- Telekomünikasyon Dinleme ve Verinin İzlenmesi (Örneğin; E-posta)[ ]  D09- Bilgisayar Kötüye Kullanımı[ ]  D10- Elektronik Delil Toplama[ ]  D11- Sızma Testi[ ]  D12- Uluslararası ve Ulusal Sektöre Özgü Şartlar (Örneğin; Bankacılık)[ ]  Diğer *(lütfen belirtiniz)*       |
| **A2. Süreçler ve Görevler** |
| **BGYS Kapsamındaki Süreçlerinizi Belirtiniz.**      |
| **BGYS Kapsamındaki Süreçleriniz İçin Aşağıdaki Tanımlamalardan Hangisi Firmanıza En Uygundur?** |
| Süreçler için seçim yapınız:[ ]  Standart ve tekrar eden görevler için standart süreçler[ ]  Standart ama tekrarı olmayan süreçler[ ]  Karmaşık süreçler | Ürün/hizmetler için seçim yapınız:[ ]  Az ürün ve/veya hizmet[ ]  Yüksek miktarda ürün ve/veya hizmetler |
| **A3. Yönetim Sistemi Kurulumunun Seviyesi, BGYS’nin Önceden Gösterdiği Performans** |
| **Firmanızda BGYS Kapsamında Politika Oluşturuldu mu?** [ ]  Evet [ ]  Hayır |
| **Firmanızda BGYS Kapsamında Organizasyon Yapısı ve Görev Tanımlamaları/Görevlendirmeler Yapıldı mı?**[ ]  Evet [ ]  Hayır*Evet, ise ne zaman ve kaç birimin görev tanımı oluşturulduğunu belirtiniz.*      |
| **Firmanızda BGYS Kapsamında Oluşturulan Prosedürler Nelerdir?** *Lütfen belirtiniz.*      |
| **Firmanızda BGYS kapsamında Bir Eğitim Planlaması Yapılmakta mıdır?**[ ]  Evet [ ]  Hayır*Evet, ise gerçekleşen eğitimler ve tarihleri nelerdir?*       |
| **Risk Değerlendirme Metodu ve Risk İşleme Süreci Tanımlanmış mıdır?**[ ]  Evet [ ]  Hayır*Evet, ise doküman adları ile revizyon numarası ve tarihini belirtiniz.*       |
| **Uygulanabilirlik Bildirgesi Tarih/Rev. No.:**      | **BGYS Risk Analiz Tarihi/Rev. No.:**      |
| **ISO 27001 Sistemlerinizin Faaliyete Geçtiği Tarih:**      | **Kapsam Dışı Maddeler (ISO 27001 Ek-A) ve Gerekçeleri:**      |
| **B1. Bilgi Teknolojileri Altyapısının Karmaşıklığı** |
| **Server (Sunucu) Sayısı (Fiziki ve Sanal):**      | **Varsa Felaket Kurtarma Merkezi (FKM) Sayısı:**      |
| **Kullanılan Bilgi Teknolojileri Platformları:**      | **Kullanılan İşletim Sistemleri:**      |
| **Veri Tabanları:**      | **Lokal ve Uzaktan Erişimli Ağ Sayısı:**      |
| **Bilgi Sistemleri Altyapısındaki Kritik Varlıklarınız (Örneğin; Autocad, İnsan, Çizim, Scada vb.):**      |
| **Bilgi Sistemleri Altyapısındaki Erişilebilirlik Gereksinimi Seviyesini Belirtiniz.**[ ]  Düşük [ ]  Orta [ ]  Yüksek |
| **Bilgi Sistemleri Altyapısında 7/24 Müşterilere Sağlanan Hizmetleriniz Var mı?**[ ]  Evet [ ]  Hayır*Evet, ise lütfen bilgi veriniz.*       |
| **B2. Dış Kaynak Kullanımı ve Tedarikçilere Bağımlılık** |
| **Dış Kaynaklara ve Tedarikçilere Bağımlılık Seviyeniz Nedir?**[ ]  Dış kaynaklara ya da tedarikçilere az ya da hiç bağımlılık[ ]  Dış kaynaklara ya da tedarikçilere bir miktar bağımlılık (bir kısım önemli iş faaliyetleriyle bağımlılık olup hepsiyle olmayan)[ ]  Dış kaynaklara ya da tedarikçilere yüksek bağımlılık (önemli iş faaliyetlerine büyük etkiye sahip tedarikçilere ya da dış kaynaklara aşırı bağımlılık) |
| **B3. Bilgi Sistemleri Gelişimi** |
| **Bilgi Sistemleri Gelişimi İçin Aşağıdaki Tanımlamalardan Hangisi Firmanıza En Uygundur?**[ ]  Kurum içi sistem/uygulama gelişiminin hiç olmaması ya da sınırlı olması[ ]  Bazı önemli iş amaçları için bazı kurum içi ya da dış kaynaklı sistem/uygulama gelişimi[ ]  Önemli iş amaçları için kurum içi ya da dış kaynaklı yoğun sistem/uygulama gelişimi |
| **C. Diğer Bilgiler** |
| **Belgelendirme Kapsamı Dışı Prosesleriniz/Faaliyetleriniz Var mı?** [ ]  Evet [ ]  Hayır*Evet, ise lütfen bu proseslerinizin/faaliyetlerinizin neler olduğunu açıklayınız.*       |
| *Yukarıdaki soruya “Hayır” işaretlediyseniz bu soruyu cevaplamayınız.***Kapsam Dışı Prosesler ve Bu Proseslerle İlgili Bağlantı Noktaları/Lokasyonlar Risk Analizine Konu Edildi mi?**[ ]  Evet [ ]  Hayır*Hayır, ise lütfen açıklayınız.*       |
| **Bilgi Teknolojileri Çalışan Sayıları *(Lütfen belirtiniz)*:**Bilgi Teknolojileri (IT) Biriminde Toplam Çalışan Sayısı :      Varsa Yazılım Geliştirme Ekibindeki Çalışan Sayısı :      Sistem Yöneticisi, Network Yöneticisi ve Veritabanı Yöneticisi Toplam Sayısı :      Bilgi Teknolojileri İle İlgili Çalışan Destek Personel Sayısı :       |
| **Teknolojik Alanlarınız (Kullandığınız Teknolojiler) Nelerdir? *(Lütfen işaretleyiniz)*:** |
| [ ]  T01- Sunucu ve Masaüstü İşletim Sistemleri[ ]  T02- Ağ ve Ağ Sistemleri[ ]  T03- Teknik Açıklık Analizi (Özellikle Dışarıya Açık Olan Hiz.)[ ]  T04- Uygulama Platformları[ ]  T05- Veri Tabanı Sistemleri (Müşteri Verileri, Üretim Verileri, Satış Verileri, Vatandaşlık Bilgileri vb.)[ ]  T06- Fiziki Güvenlik Tedbirleri[ ]  T07- Mesajlaşma Güvenliği[ ]  T08- Kriptografik Kontrollerin Düzenlenmesi[ ]  T09- Elektronik Ticaret[ ]  T10- Otomasyon Sistemi | [ ]  T11- Üretim Aşamalarında Alınan Bilgi Güvenliği Tedbirleri (Çizimler, Projeler, Formüller vb.)[ ]  T12- Hizmet Aşamalarında Alınan Bilgi Güvenliği Tedbirleri (Müşteri Bilgileri vb.)[ ]  T13- Yazılım Kodlama Teknikleri[ ]  T14- E-Fatura[ ]  T15- E-Arşiv[ ]  T16- E-Defter[ ]  T17- 3D Secure[ ]  T18- Bulut Bilişim[ ]  Diğer *(lütfen belirtiniz)*       |
| **BGYS Kapsamında Gizlilik Oluşturan ve CTR ile Paylaşılamayacak Gizli ve Hassas Bilgi (Maaş Bilgisi, Personel Özel Bilgileri, Ar-Ge, Tasarım, Finansal Bilgiler vb.) İçeren Kayıtlar Var mı?**[ ]  Var [ ]  Yok*Var, ise lütfen açıklayınız.*       |
| **BGYS Kapsamında Yer Alan Ama Denetimde Kanıt/Kayıt Gösteremeyeceğiniz, Bakmamızı İstemeyeceğiniz Özel Bölümleriniz, Uygulamalarınız, Tesisleriniz vb. Var mı? (3)**[ ]  Var [ ]  Yok*Var, ise lütfen açıklayınız.*      ***(3)*** *Gizli ya da hassas kayıtları incelemeden BGYS*’nin *uygun bir şekilde denetiminin yapılmasının mümkün olmadığı durumlarda uygun erişim düzenlemeleri sağlanana kadar belgelendirme denetimi gerçekleştirilemez.* |
| **BGYS Kapsamında Ziyaret Etmemiz Gereken Başka Yerler Var mı (Data Center, Yazılım Geliştirme, Tekno Park, Ar-Ge Ofisleri vb.)?**[ ]  Var [ ]  Yok*Var, ise lütfen lokasyonları ile birlikte açıklayınız.*       |
| **Elektrik Piyasası Lisans Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik kapsamına Giriyorsa ISO 27019’a Göre Raporlama İsteniyor mu?**[ ]  Evet [ ]  Hayır |
| **D. Saha Bilgileri** |
| **Sahalar** | **Kuruluş Merkezi** | **Saha 1** | **Saha 2** | **Saha 3** |
| Sahadaki kritik varlıklar (Bilgi sistemleri vb.) |       |       |       |       |
| Yönetim sistemi kapsamındaki risk öncelikli prosesler |       |       |       |       |
| Bilgi güvenliği olayı yaşanmış herhangi bir saha var mı? | [ ]  Evet [ ]  Hayır*Açıklayınız*       | [ ]  Evet [ ]  Hayır*Açıklayınız*       | [ ]  Evet [ ]  Hayır*Açıklayınız*       | [ ]  Evet [ ]  Hayır*Açıklayınız*       |

*\*\*\* Daha fazla saha var ise bu sayfanın ekinde yukarıdaki şablona uygun bir doküman ekleyiniz.*

|  |
| --- |
| ***YALNIZCA ISO 27701 BAŞVURULARI İÇİN:*** |
| **ISO 27701 Sisteminizin Faaliyete Geçtiği Tarih:**      | **Kapsam Dışı Maddeler (ISO 27701 Ekleri) ve Gerekçeleri:**      |
| **Lütfen kişisel verinin korunması kapsamında kuruluşunuzun türünü belirtiniz.** |
| Veri Sorumlusu [ ]  | Veri İşleyen [ ]  |
| ***Not 1:****- Veri sorumlusu firmalar sadece kendi çalışanlarının ve varsa gerekli durumlarda müşterilere ait kişisel verileri saklayan firmalar (Örneğin üretim yapan kuruluşlar)**- Veri işleyen firmalar ise; veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişilerin bilgilerini tutan firmalardır. (Örnek: kargo şirketleri, hastaneler, oteller, turizm acenteleri vb.)* |