

Risk Değerlendirme Çalışması

Bilgi İşlem Dairesi Başkanlığımız 2022 yılı içerisinde, bilgi güvenliği kapsamında iç ve dış süreçlerin işleyişinde ISO 27001 Bilgi Güvenliği Yönetim Sistemi standartlarına ulaşmayı hedefleyerek yola çıkmış; 24-27 Mayıs tarihleri arasında birimizde Türk Standartları Enstitüsü tarafından gerçekleştirilen Temel Bilgi Güvenliği Eğitimi, Belge ve Dokümantasyon Eğitimi, İç Tetkik eğitimlerini tüm personelin katılımı ile tamamlamıştır. Birimiz, standartlaşma sürecinin ilk adımı olarak ISO 27001 standardı maddelerini uygulamaya geçirmek için bilgi güvenliği ile ilgili süreçleri yazılı hale getirmiştir. Öncelikli olarak kurum organizasyon şeması ve görev grupları belirlenmiş ve mevcut personeller ile ilişkilendirilmiştir.

Her birimin yıl içindeki hedefleri, bu hedeflere ulaşmak için yapılması gereken faaliyetler, ayrılması gereken kaynaklar, termin tarihi ve gerçekleştirme ölçütü yazılı halde oluşturulmuştur.

Bilgi güvenliği risk faktörleri, ISO 27001 Risk Değerlendirme standartları esas alınarak risk işleme tablosunda yazılı hale getirilmiştir. Bu tabloda, birim içindeki bilginin bütünlüğü, erişilebilirliği ve gizliliği nicel olarak belirtilmiş, ihlal olasılıkları tanımlanmış ve risk faktörlerinin kurum için oluşturabileceği etkiler değerlendirilmiştir.

Risk değerlendirme tablosuna bağlı olarak risk işleme süreci ve ihlal olaylarının gerçekleşmesi durumunda uygulanacak düzeltici ve önleyici faaliyetler, yıl içindeki rutin tatbikatlar aynı şekilde risk ve süreç işleme tablolarında yazılı hale getirilmiştir.

Birim içindeki işleyişin ISO 27001 standartlarına uygun hale getirilebilmesi için bilgi güvenliği politikaları tanımlanmış ve yazılı hale getirilmiştir. Aynı şekilde talimatlar, politikalar ve prosedürler oluşturulmuştur. İş sürekliliği ve etkinlik ölçüm çizelgeleri oluşturulmuştur.

Daire Başkanlığımız Bilgi güvenliği yönetim sistemi standartlaşma süreci 2022 yılı Ekim ayı itibari ile tamamlanmış; yapılan denetim çalışması sonucunda ISO 27001;2017 Bilgi güvenliği Yönetim Sistemi Standardı belgesini almaya hak kazanmıştır. Denetim sırasında minör hatalar tespit edilmiş olup bunlar içerisinde "Risk Değerlendirme" çalışmasına da yer verilmiştir.

ISO 27001;2017 Dokümanları listesi, Web Sayfamızda Raporlar ve Formlar başlığı altında bulunmaktadır. Ayrıca Daire Başkanlığımızda Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi kapsamında çalışmalar devam etmektedir.

ISO 27001 için belirlenen Minör kusur olan "Risk Değerlendirme" çalışması, DDO rehberi ile birlikte ele alınmak üzere çalışmalar başlatılmıştır.