ISO/IEC 27001-2022 Bilgi Güvenliği Yönetim Sistemi Versiyon Geçiş Planı

Standart Maddesi		Planlanan Aktivite	İlgili Doküman ve/veya Kayıt	Aktivite Sonucu
4 Kuruluşun bağlamı				
4.1	Kuruluş ve bağlamının anlaşılması			
4.2	İlgili tarafların ihtiyaç ve beklentilerinin anlaşılması			
4.3	Kalite yönetim sisteminin kapsamının belirlenmesi			
4.4	Kalite yönetim sistemi ve prosesleri			
5 Liderlik				
5.1	Liderlik ve taahhüt			
5.2	Politika			
5.3	Kurumsal görev, yetki ve sorumluluklar			
6 Planlama				
6.1	Risk ve fırsatları belirleme faaliyetleri			
6.2	Kalite amaçları ve bunlara erişmek için planlama			
6.3	Değişikliklerin planlanması			
7 Destek				
7.1	Kaynaklar			
7.2	Yeterlilik			
7.3	Farkındalık			
7.4	İletişim			
7.5	Dokümante edilmiş bilgi			

Standart Maddesi		Planlanan Aktivite	İlgili Doküman ve/veya Kayıt	Aktivite Sonucu
8 Operasyon				
8.1	Operasyonel planlama ve kontrol			
8.2	Ürün ve hizmetler için şartlar			
8.3	Ürün ve hizmetlerin tasarımı ve geliştirilmesi			
8.4	Dışarıdan tedarik edilen proses, ürün ve hizmetlerin kontrolü			
8.5	Üretim ve hizmetin sunumu			
8.6	Ürün ve hizmet sunumu			
8.7	Uygun olmayan çıktının kontrolü			
9 Performans değerlendirme				
9.1	İzleme, ölçme, analiz ve değerlendirme			
9.2	İç tetkik			
9.3	Yönetimin gözden geçirmesi			
10 İyileştirme				
10.1	Genel			
10.2	Uygunsuzluk ve düzeltici faaliyet			
10.3	Sürekli iyileştirme			

Kontrol Maddeleri	Planlanan Aktivite	İlgili Doküman ve/veya Kayıt	Aktivite Sonucu
5 ORGANİZASYONEL KONTROLLER			
5.1 Bilgi güvenliği için politikalar			
5.2 Bilgi güvenliği rolleri ve sorumlulukları			
5.3 Görevler ayrılığı			
5.4 Yönetim sorumluluğu			
5.5 Otoritelerle iletişim			
5.6 Özel ilgi grupları ile iletişim			
5.7 Tehdit araştırma			
5.8 Proje yönetiminde bilgi güvenliği			
5.9 Bilgi ve diğer ilişkili varlıkların envanteri			
5.10 Bilgi ve diğer ilgili varlıkların kabul edilebilir kullanımı			
5.11 Varlıkların iadesi			
5.12 Bilginin sınıflaması			
5.13 Bilginin etiketlenmesi			
5.14 Bilgi transferi			
5.15 Erişim kontrol			
5.16 Kimlik yönetimi			
5.17 Kimlik denetleme bilgisi			
5.18 Erişim hakları			
5.19 Tedarikçi ilişkilerinde bilgi güvenliği			
5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin adreslenmesi			
5.21 Bilgi ve iletişim teknoloji tedarik zincirinde bilgi güvenliğinin yönetimi			

Kontrol Maddeleri	Planlanan Aktivite	İlgili Doküman ve/veya Kayıt	Aktivite Sonucu
5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişim yönetimi			
5.23 Bulut hizmetlerinin kullanımında bilgi güvenliğinin kullanımı			
5.24 Bilgi güvenliği vaka yönetim planlaması ve hazırlığı			
5.25 Bilgi güvenliği ihlal değerlendirmesi ve karar verilmesi			
5.26 Bilgi güvenliği vakalarına müdahale etme			
5.27 Bilgi güvenliği vakalarından çıkarılan dersler			
5.28 Delillerin toplanması			
5.29 Kesinti süresince bilgi güvenliği			
5.30 Bilgi ve iletişim teknolojilerinin iş sürekliliğine hazır olması			
5.31 Yasal, meşru, düzenleyici ve sözleşmesel şartlar			
5.32 Fikri ve mülki haklar			
5.33 Kayıtların korunması			
5.34 Kişisel verilerin mahremiyeti ve korunması			
5.35 Bilgi güvenliğinin bağımsız gözden geçirilmesi			
5.36 Bilgi güvenliği politikalarına, kurallarına ve standartlarına uyum			
5.37 Dokümante edilmiş operasyon prosedürleri			
6 KİŞİLERİN KONTROLÜ			
6.1 İzleme			

Kontrol Maddeleri	Planlanan Aktivite	İlgili Doküman ve/veya Kayıt	Aktivite Sonucu
6.2 İşe alma kural ve şartları			
6.3 Bilgi güvenliği farkındalık, öğrenim ve eğitimi			
6.4 Disiplin süreçleri			
6.5 İş akdinin iptali veya değiştirilmesinin ardından sorumluluklar			
6.6 Gizlilik veya gizlilik anlaşmaları			
6.7 Uzaktan çalışma			
6.8 Bilgi güvenliği olay raporlama			
7 FİZİKSEL KONTROLLER			
7.1 Fiziksel güvenlik ölçütleri			
7.2 Fiziksel giriş			
7.3 Ofis, odalar ve yerleşkenin güvenliği			
7.4 Fiziksel güvenlik izlemesi			
7.5 Fiziksel e çevresel tehditlere karşı koruma			
7.6 Güvenli alanlarda çalışma			
7.7 Temiz masa temiz ekran			
7.8 Ekipman yerleşimi ve koruması			
7.9 Yerleşke dışındaki ekipmanların güvenliği			
7.10 Depolama ortamı			
7.11 Destek tesisler			
7.12 Kablolama güvenliği			
7.13 Ekipman bakımı			
7.14 Ekipmanların güvenli elden çıkarılması veya tekrar kullanımı			
8 TEKNOLOJİK KONTROLLER			
8.1 Son kullanıcı aletleri			

Kontrol Maddeleri	Planlanan Aktivite	İlgili Doküman ve/veya Kayıt	Aktivite Sonucu
8.2 Ayrıcalıklı erişim hakları			
8.3 Bilgi erişim kısıtlamaları			
8.4 Kaynak kodlarına erişim			
8.5 Güvenli kimlik denetimi			
8.6 Kapasite yönetimi			
8.7 Kötücül yazılıma karşı koruma			
8.8 Teknik zafiyetlerin yönetimi			
8.9 Konfigürasyon yönetimi			
8.10 Bilgi silinmesi			
8.11 Veri maskeleme			
8.12 Veri sızıntı koruma			
8.13 Bilgi yedekleme			
8.14 Bilgi işleme tesislerinin fazlalıkları			
8.15 Loglama			
8.16 İzleme faaliyetleri			
8.17 Saat senkronizasyonu			
8.18 Ayrıcalıklı hizmet programlarının kullanımı			
8.19 İşletim sistemlerine yazılım yükleme			
8.20 Ağ güvenliği			
8.21 Ağ hizmetlerinin güvenliği			
8.22 Ağların ayrımı			
8.23 Web filtreleme			
8.24 Kriptografi kullanımı			
8.25 Güvenli geliştirme yaşam döngüsü			
8.26 Güvenlik şartlarının uygulanması			
8.27 Güvenli sistem mimarisi ve mühendislik prensipleri			

Kontrol Maddeleri	Planlanan Aktivite	İlgili Doküman ve/veya Kayıt	Aktivite Sonucu
8.28 Güvenli kodlama			
8.29 Geliştirme ve kabullerde güvenlik testleri			
8.30 Dış kaynakla geliştirme			
8.31 Geliştirme, test ve üretim ortamlarının ayrılması			
8.32 Değişim yönetimi			
8.33 Test bilgisi			
8.34 Tetkik testlerinde bilgi güvenliğinin korunması			

Geçiş Planını Hazırlayanın İsmi	
Tarih	
İmza	