# *SC-400T00: Microsoft Information Protection Administrator*

Microsoft 365 kurulumunuzdaki bilgilerin nasıl korunacağını öğrenin. Bu eğitim, kuruluşunuzdaki veri yönetişimine ve bilgilerin korunmasına odaklanmaktadır. Eğitim, ilgili diğer konu başlıkları ile beraber veri kaybını önleme politikalarının uygulamaya konulmasını, hassas bilgi türlerini, hassaslık etiketlerini, veri saklama politikalarını ve Office 365'in mesaj şifrelemesini kapsamaktadır. Bu eğitim, öğrencilerin Microsoft Bilgi Koruma Yöneticisi sınavına (SC-400) hazırlanmalarına yardımcı olmaktadır.

**Hedefler**

- Hassas etiketleri açıklama ve kullanma.
- Veri Kaybını Önleme politikalarını yapılandırma.
- Office 365'de mesajları güvenli hale getirme.
- Bilgi yönetişimi yapılandırma sürecini açıklama.
- Microsoft'un bilgi koruma ve yönetişim çözümleriyle ilişkili temel terimleri tanımlama.
- İçerik gezginini ve Etkinlik gezginini açıklama.
- Hassas bilgi türlerinin ve eğitilebilir sınıflandırıcıların nasıl kullanıldığını açıklama.
- DLP raporlarını gözden geçirme ve analiz etme.
- DLP politikası ihlallerini belirleme ve azaltma.
- DLP'nin Microsoft Bulut Uygulama Güvenliği (MCAS) ile entegrasyonunu açıklama.
- Endpoint DLP'yi kurma.
- Kayıt yönetimini açıklama.

- Olay odaklı elde tutmayı yapılandırma.
- Dosya planını içe aktarma.
- Elde tutma politikaları ve etiketlerini yapılandırma.
- Özel anahtar kelime sözlüklerini oluşturma.
- Doküman parmak izi kontrolünü uygulamaya koyma.

**Hedef Kitle**

Bilgi Koruma Yöneticisi, kuruluşun uyum ihtiyaçlarını karşılayan kontrolleri planlar ve uygulamaya koyar. Bu kişi, ihtiyaçların ve uyum kontrollerinin teknik uygulamaya çevrilmesinden sorumludur. Kuruluşların kontrol sahiplerinin uyumlu olmalarına ve bu şekilde kalmalarına yardımcı olurlar. Kuruluşlarının yasal gereksinimlerini yeterli seviyede karşılamak için gereken politikaları ve kontrolleri destekleyen teknolojiyi uygulamaya koymak için bilgi teknolojisi (BT) personeliyle, iş uygulaması sahipleriyle, insan kaynaklarıyla ve yasal paydaşlarla birlikte çalışırlar. Ayrıca ilişkili kurumsal riski her yönüyle değerlendirmek için Uyum Yöneticisi ve Güvenlik Yöneticisi gibi uyum ve güvenlik liderleriyle ve bu politikaların geliştirilmesi için de ilgili iş ortağıyla birlikte çalışırlar. Bu kişi, BT'nin işleme koyduğu ilgili gereksinimleri ve testleri ve bu politika ve kontrollerin uygulamalarını tanımlar. Ayrıca içerik sınıflandırma, veri kaybını önleme, yönetişim ve koruma ileilgili politika ve kuralların oluşturulmasından da sorumludurlar.

**Topics**

- Implement Information Protection in Microsoft 365
- Implement Data Loss Prevention in Microsoft 365
- Implement Information Governance in Microsoft 365