1. Giriş

ISO 27001:2022 standardı, bilgi güvenliği yönetim sistemlerinin kurulması ve sürdürülmesi için bir çerçeve sunar. Bulut hizmetlerinin yaygınlaşmasıyla birlikte, bu hizmetlerin kullanımıyla ilgili risklerin yönetimi büyük önem kazanmıştır. Bu prosedür, Kurumların bulut hizmetlerini kullanırken bilgi güvenliğini sağlamalarına yardımcı olmak amacıyla hazırlanmıştır.

2. Amaç

Bu prosedürün amacı, Kurumun bulut hizmetlerini kullanırken bilgi varlıklarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için gerekli güvenlik kontrollerini tanımlamak ve uygulamakdır.

3. Kapsam

Bu prosedür, Kurumun kullandığı tüm bulut hizmetlerini kapsar. Bulut hizmet sağlayıcısı (CSP) ile yapılan sözleşmelerin değerlendirilmesi, bulut ortamında veri güvenliği, erişim kontrolü, veri yedekleme ve felaket kurtarma gibi konuları içerir.

4. Sorumluluklar

Bilgi Güvenliği Yöneticisi: Prosedürün uygulanmasından genel olarak sorumludur.

Bulut Hizmetleri Yöneticisi: Bulut hizmetlerinin seçimi, konfigürasyonu ve yönetiminden sorumludur.

Bilgi Güvenliği Ekibi: Bulut ortamında güvenlik risklerinin değerlendirilmesi ve uygun güvenlik kontrollerinin uygulanmasından sorumludur.

5. Uygulama

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

5.1.Bulut Hizmeti Sağlayıcısı (CSP) Değerlendirmesi

CSP'nin ISO 27001 sertifikasına sahip olup olmadığının kontrol edilmesi.
CSP'nin güvenlik politikalarının ve prosedürlerinin incelenmesi.
CSP'nin sunduğu güvenlik hizmetlerinin Kurumun ihtiyaçlarına uygunluğunun değerlendirilmesi.
CSP ile hizmet seviyesi anlaşması (SLA) müzakereleri.

5.2.Veri Sınıflandırması ve Etiketleme

Bulut ortamında saklanan verilerin hassasiyet seviyesine göre sınıflandırılması.
Verilere erişim yetkilerinin role ve göreve göre belirlenmesi.
Verilerin şifrelenmesi ve güvenli bir şekilde aktarılması.

5.3.Erişim Kontrolü

Kimlik doğrulama ve yetkilendirme mekanizmalarının kurulması.
Çok faktörlü kimlik doğrulama (MFA) kullanımının teşvik edilmesi.
Erişim loglarının tutulması ve düzenli olarak incelenmesi.

5.4.Veri Yedekleme ve Felaket Kurtarma

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

Verilerin düzenli olarak yedeklenmesi ve yedeklerin güvenli bir ortamda saklanması.
Felaket durumunda verilerin hızlı bir şekilde kurtarılması için planların hazırlanması.

5.5.Güvenlik Olayları Yönetimi

Güvenlik olaylarının tespiti, analizi ve yanıtlanması için süreçlerin oluşturulması.
Güvenlik olaylarının raporlanması ve kök neden analizinin yapılması.

5.6.Güvenlik Farkındalığı Eğitimi

Çalışanlara bulut hizmetleri kullanımıyla ilgili güvenlik farkındalığı eğitimleri verilmesi.

5.7.Sürekli İyileştirme

Bulut güvenliği risklerinin düzenli olarak değerlendirilmesi ve prosedürün güncellenmesi.
CSP tarafından sunulan yeni güvenlik özelliklerinin değerlendirilmesi.

6. Ölçüm ve İzleme

Bulut hizmetleri kullanımına ilişkin metriklerin toplanması ve analiz edilmesi.
Güvenlik olaylarının sayısı ve türü gibi göstergelerin takip edilmesi.
Uygunsuzlukların tespiti ve düzeltici faaliyetlerin gerçekleştirilmesi.

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı