

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bulut Hizmetleri Yönetim Prosedürü	Doküman No	PR-036
		İlk Yayın Tarihi	29.09.2025
		Revizyon Tarihi	29.09.2025
		Revizyon No	000
		Sayfa No	1 / 3

1. AMAÇ

Bu prosedürün amacı, kuruluşun kullandığı veya kullanmayı planladığı bulut hizmetlerinin edinimi, kullanımı, yönetimi ve bulut hizmetlerinden çıkış süreçlerinin bilgi güvenliği gerekliliklerine uygun olarak yönetilmesini sağlamaktır.

2. KAPSAM

Bu prosedür, kuruluşun tüm iş birimlerini, bilgi sistemlerini, uygulamalarını ve bulut hizmet sağlayıcıları ile olan ilişkilerini kapsar.

3. SORUMLULAR

- Satın alma Birimi:** Tedarikçi seçiminde güvenlik gereksinimlerinin karşılanmasını sağlamak.
- Sistem Yöneticileri:** Bulut hizmeti üzerindeki erişim, loglama ve konfigürasyonları yönetmek.
- Kullanıcılar:** Bulut hizmetlerini yalnızca yetkilendirilmiş amaçlar doğrultusunda kullanmak.

4. TANIMLAR

4.1. Bulut Hizmetleri: İnternet üzerinden sağlanan ve kullanıcıların uzak sunucular üzerinde veri saklama, işleme ve diğer bilişim hizmetlerinden yararlanmasına olanak tanıyan hizmetler.

5. UYGULAMA

5.1. Bulut Hizmeti Edinimi

- Bulut hizmeti satın almadan önce gerekli araştırma yapılarak teknik şartname hazırlanır.
- Hizmet sağlayıcının sertifikaları (ISO 27001, SOC 2 vb.), veri merkezi konumu, SLA şartları incelenir.
- Bulut hizmet sağlayıcılarıyla yapılan sözleşmeler, bilgi güvenliği gereksinimlerini ve hizmet düzeyi anlaşmalarını (SLA) içerir. Bu anlaşmalar, veri güvenliği, erişim kontrolü ve olay yönetimi gibi konuları kapsar.
- Bulut hizmet sağlayıcılarının seçimi öncesinde risk değerlendirmesi yapılır. Bu değerlendirme, hizmet sağlayıcının güvenlik standartları, uyumluluk durumu ve hizmetin güvenliğini etkileyen faktörleri içerir.

5.2. Bulut Hizmetlerinin Kullanımı ve Yönetimi

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekai KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bulut Hizmetleri Yönetim Prosedürü	Doküman No	PR-036
		İlk Yayın Tarihi	29.09.2025
		Revizyon Tarihi	29.09.2025
		Revizyon No	000
		Sayfa No	2 / 3

- Bulut hizmetlerine erişim, yetki matrisi çerçevesinde yalnızca gerekli kişilerle sınırlandırılır.
- Bulut sistemlerine erişim, rol ve sorumluluk temelli (RBAC) veya en az ayrıcalık prensibine göre düzenlenir. Kullanıcı kimlik doğrulaması ve çok faktörlü kimlik doğrulama (MFA) yöntemleriyle ek güvenlik sağlanır. Kritik veriler bulut ortamında şifreli olarak saklanır ve iletilir.
- Üniversite verileri, gizlilik derecelerine göre (kamusal, kurumsal, gizli vb.) sınıflandırılır ve uygun güvenlik önlemleri uygulanır. Bulut ortamında saklanan veya işlenen tüm veriler, yetkisiz erişime, sızmaya, değiştirmeye veya kayba karşı korunur. Bulut bilişim hizmetleri düzenli olarak risk değerlendirmesine tabi tutulur; belirlenen risklere karşı önlemler alınır.
- Bulut ortamında saklanan ve iletilen veriler, organizasyonun güvenlik politikalarına uygun olarak şifrelenir. Şifreleme yöntemleri, veri güvenliğini sağlamak için güncel standartlara uygun olmalıdır.
- Verilerin düzenli olarak yedeklenmesi sağlanır. Yedekleme işlemleri, bulut hizmet sağlayıcısının politikalarına uygun olarak yapılır ve yedekleme verilerinin güvenliği sağlanır.
- Bulut servis sağlayıcılarının sunduğu güvenlik logları, izleme ve denetim özellikleri düzenli olarak takip edilir. Olası zafiyetleri tespit etmek ve güvenlik seviyesini artırmak amacıyla penetrasyon testleri, zafiyet taramaları ve iç/dış denetimler yapılır. SLA performansı yılda en az bir kez gözden geçirilir.
- Üçüncü taraf bulut hizmet sağlayıcılarıyla yapılan tüm sözleşmelerde veri gizliliği, bütünlüğü, erişilebilirliği ve ilgili yasal düzenlemelere uyum şartları açıkça belirtilir. Hizmet sözleşmelerinde kişisel verilerin korunması (KVKK), uluslararası mevzuat (örneğin GDPR) ve telif hakları gibi düzenlemeler gözetilir.
- Bulut ortamıyla ilgili meydana gelen güvenlik ihlalleri veya olayları için olay yönetim prosedürleri uygulanır. Güvenlik olayları en kısa sürede Bilgi İşlem daire başkanlığına bildirilir ve gereken aksiyonlar alınır.
- Bulut hizmetlerini kullanan tüm çalışanlara, bulut güvenliği ve bilgi güvenliği konularında düzenli eğitimler verilir. Bulut hizmetleri ve bilgi güvenliği konularında bilinçlendirme faaliyetleri düzenlenir.

5.3. Bulut Hizmetlerinden Çıkış (Exit Plan)

- Hizmetin sonlandırılması durumunda veri, önceden tanımlanan formatta güvenli şekilde alınır.
- Hizmet sağlayıcıdan verilerin silindiğine dair kanıt (sertifika, rapor) talep edilir.
- Çıkış sonrası erişim yetkileri derhal iptal edilir.
- Çıkış süreci raporlanır ve dosyalanır.

6. İLGİLİ DOKÜMANLAR

- PR-018 Satın Alma ve İhale Prosedürü

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekai KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bulut Hizmetleri Yönetim Prosedürü	Doküman No	PR-036
		İlk Yayın Tarihi	29.09.2025
		Revizyon Tarihi	29.09.2025
		Revizyon No	000
		Sayfa No	3 / 3

- PR-004 Olay İhlal Prosedürü

7. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	29.09.2025	İlk yayın.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekai KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI