1. AMAÇ

Bu prosedürün amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS**)** kapsamında kullanılan veya kullanılması planlanan bulut hizmetlerinin; bilgi güvenliği, kişisel verilerin korunması, iş sürekliliği, hizmet yönetimi ve ilgili mevzuat şartlarına uygun olarak değerlendirilmesi, edinilmesi, kullanılması, yönetilmesi, izlenmesi ve sonlandırılması için uygulanacak usul ve esasları belirlemektir.

2. KAPSAM

Bu prosedür; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilinde kullanılan veya kullanılması planlanan bulut hizmetlerini, bu hizmetlerde işlenen Üniversite bilgi varlıklarını, kullanıcıları, bilgi sistemlerini ve bulut hizmet sağlayıcıları ile yürütülen ilişkileri kapsar.

Prosedür; bulut hizmetlerinin edinilmesi, hizmet sağlayıcı seçimi, risk değerlendirmesi, sözleşme ve hizmet seviyesi şartlarının belirlenmesi, erişim yetkilendirmesi, veri güvenliği, izleme, yedekleme, güvenlik olaylarının yönetimi ve hizmetten çıkış süreçlerini kapsar.

3. SORUMLULAR

- **Yönetim Temsilcisi:** Prosedürün uygulanmasını ve EYS ile uyumunu takip etmek.
- **Bilgi İşlem Daire Başkanlığı:** Bulut hizmetlerinin teknik, erişim ve bilgi güvenliği kontrollerini yürütmek.
- **İlgili Birim:** Bulut hizmetinin kullanım ihtiyacını, kullanıcılarını ve hizmete ilişkin gereklilikleri belirlemek.
- **Kullanıcılar:** Bulut hizmetlerini kendilerine verilen yetkiler ve Üniversite düzenlemelerine uygun kullanmak.

4. TANIMLAR

- ***Bulut Hizmeti:*** İnternet veya elektronik iletişim ağları üzerinden, Üniversitenin kendi bilgi teknolojisi altyapısı dışında bulunan kaynaklardan bilişim hizmeti, veri depolama, veri işleme, yazılım, platform veya altyapı hizmetlerinin sunulmasını ifade eder.
- ***Bulut Hizmet Sağlayıcısı:*** Bulut hizmetini Üniversiteye sunan üçüncü taraf kuruluşu ifade eder.
- ***Hizmet Seviyesi Anlaşması (SLA):*** Bulut hizmet sağlayıcısı tarafından sunulacak hizmetin kapsamını, kullanılabilirlik, performans, destek, müdahale ve benzeri hizmet seviyelerini belirleyen anlaşmayı ifade eder.
- ***Çıkış Planı (Exit Plan):*** Bulut hizmetinin sonlandırılması veya başka bir hizmet sağlayıcıya geçilmesi durumunda verilerin alınması, aktarılması, silinmesi, erişimlerin sonlandırılması ve hizmetten güvenli şekilde çıkılması için uygulanacak planı ifade eder.
- ***EYS:*** Süleyman Demirel Üniversitesi Entegre Yönetim Sistemini ifade eder.

5. UYGULAMA

5.1. Bulut Hizmetinin Talep Edilmesi ve Ön Değerlendirme

Üniversite bünyesinde yeni bir bulut hizmetinin kullanılması planlandığında, öncelikle hizmetin amacı, kapsamı, iş gereksinimi ve işlenecek bilgi/verilerin niteliği belirlenir. Bulut hizmetinde işlenecek veya saklanacak verilerin Bilgi Sınıflandırma ve Etiketleme Politikası kapsamında belirlenen sınıflandırması dikkate alınır. Hizmetin Üniversite açısından oluşturabileceği bilgi güvenliği, kişisel veri, iş sürekliliği ve hizmet sürekliliği riskleri değerlendirilir.

Hizmet sağlayıcının aşağıdaki hususları değerlendirmeye alınır:

- Bilgi güvenliği ve kişisel verilerin korunmasına ilişkin uygulamaları,
- Sahip olduğu ilgili sertifikalar ve bağımsız denetim raporları,
- Veri işleme ve veri saklama konumları,
- Erişim kontrolü ve kimlik doğrulama özellikleri,
- Loglama ve izleme imkânları,
- Yedekleme ve geri yükleme imkânları,
- Hizmet sürekliliği ve felaket kurtarma yetenekleri,
- Güvenlik olaylarının bildirilmesi ve yönetimi,
- Veri aktarımı ve hizmetten çıkış imkânları,
- Hizmet seviyeleri ve destek koşulları.

Gerekli görülmesi halinde hizmet sağlayıcının bilgi güvenliği ve kişisel veri uygulamalarına ilişkin belge ve kanıtlar talep edilir.

5.2. Bulut Hizmetinin Edinilmesi

Bulut hizmetinin edinilmesine ilişkin satın alma ve tedarik süreçleri Satın Alma ve İhale Prosedürü doğrultusunda yürütülür. Bulut hizmet sağlayıcısı ile yapılacak sözleşme ve hizmet seviyesi anlaşmalarında, hizmetin niteliğine ve risk düzeyine uygun olarak aşağıdaki hususlar tanımlanır:

- Hizmetin kapsamı,
- Hizmet seviyesi ve kullanılabilirlik şartları,
- Bilgi güvenliği gereksinimleri,
- Veri gizliliği ve bütünlüğü,
- Erişim kontrolü,
- Güvenlik olaylarının bildirilmesi,
- Log ve kayıtların tutulması,
- Yedekleme ve veri kurtarma,
- İş sürekliliği,
- Alt yüklenici kullanımı,
- Kişisel verilerin korunmasına ilişkin şartlar,

- Veri saklama ve aktarım koşulları,
- Hizmet sonlandırma ve veri silme şartları.

Kişisel verilerin bulut hizmetinde işlenmesi halinde, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat kapsamında gerekli değerlendirmeler yapılır. Bulut hizmetinin Üniversitenin kritik bilgi varlıklarını veya kritik hizmetlerini etkilemesi halinde, iş sürekliliği ve bilgi güvenliği açısından gerekli ilave kontroller belirlenir.

5.3. Bulut Hizmetlerinin Kullanımı ve Yönetimi

- Bulut hizmetlerine erişim, Erişim Kontrol Politikası doğrultusunda görev ve sorumluluklar esas alınarak yetkilendirilir.
- Kullanıcıların yalnızca görevlerini yerine getirmek için ihtiyaç duydukları kaynaklara erişmeleri sağlanır ve en az ayrıcalık prensibi uygulanır.
- Bulut hizmetlerinde mümkün olduğu durumlarda çok faktörlü kimlik doğrulama (MFA) kullanılır. Kullanıcıların görev, birim veya yetki değişikliği ya da
- Üniversiteden ayrılması durumunda bulut hizmetlerine ilişkin erişim yetkileri gözden geçirilir ve gerekli erişimler kaldırılır. Bulut hizmetlerinde saklanan veya işlenen
- Üniversite bilgileri, bilgi sınıflandırma seviyesine ve risk durumuna uygun güvenlik kontrolleri ile korunur.
- Bulut hizmetlerinde kritik veya hassas bilgilerin saklanması ve aktarılması durumunda, hizmetin desteklediği ve risk değerlendirmesinde gerekli görülen şifreleme mekanizmaları kullanılır.
- Bulut hizmetlerinde kullanılan güvenlik yapılandırmaları, yetkisiz değişikliklere karşı korunur ve gerekli görülen durumlarda düzenli olarak gözden geçirilir.
- Hizmet sağlayıcının sunduğu güvenlik logları, izleme ve denetim imkânları hizmetin risk düzeyi ve kritikliği dikkate alınarak takip edilir.
- Bulut hizmetlerinde tespit edilen güvenlik zafiyetleri, ilgili zafiyet ve olay yönetimi süreçleri kapsamında değerlendirilir.
- Bulut hizmet sağlayıcısının hizmet performansı ve SLA şartlarına uygunluğu, hizmetin kritiklik düzeyine göre periyodik olarak gözden geçirilir. Gerekli görülen durumlarda hizmet sağlayıcıdan düzeltici faaliyet talep edilir.

5.4. Yedekleme ve İş Sürekliliği

- Bulut hizmetlerinde tutulan verilerin yedeklenmesine ilişkin gereksinimler, verinin kritiklik seviyesi ve hizmetin niteliğine göre belirlenir.
- Yedekleme işlemleri Üniversitenin ilgili yedekleme ve iş sürekliliği düzenlemelerine uygun olarak yürütülür.
- Kritik hizmetlerde, hizmet sağlayıcının kesinti veya erişilemezlik durumlarına karşı sunduğu iş sürekliliği ve felaket kurtarma mekanizmaları değerlendirilir.
- Gerekli görülen durumlarda veri geri yükleme ve hizmet sürekliliği senaryoları test edilir.

5.5. Bilgi Güvenliği Olaylarının Yönetimi

- Bulut hizmetlerinde meydana gelen veya meydana geldiğinden şüphelenilen bilgi güvenliği olayları, Olay İhlal Prosedürü doğrultusunda ilgili birimlere bildirilir.
- Bulut hizmet sağlayıcısının sorumluluğunda bulunan güvenlik olaylarında, sözleşmede belirlenen bildirim ve müdahale süreleri dikkate alınır.
- Olayın niteliğine göre gerekli teknik, idari ve hukuki tedbirler alınır ve olay kayıt altına alınır.

5.6. Bulut Hizmetlerinin Periyodik Gözden Geçirilmesi

- Kullanılan bulut hizmetleri; bilgi güvenliği, hizmet performansı, erişim yetkileri, veri güvenliği, mevzuat ve sözleşme şartları açısından periyodik olarak gözden geçirilir.
- Risk değerlendirmesini etkileyebilecek önemli değişiklikler, hizmet kapsamının değişmesi, güvenlik olayı, mevzuat değişikliği veya hizmet sağlayıcının değişmesi durumunda gerekli değerlendirmeler yeniden yapılır.
- Yapılan değerlendirmeler sonucunda tespit edilen uygunsuzluk ve riskler için gerekli düzeltici ve iyileştirici faaliyetler başlatılır.

5.7. Bulut Hizmetlerinden Çıkış

- Bulut hizmetinin sonlandırılması, hizmet sağlayıcının değiştirilmesi veya hizmetin artık kullanılmaması durumunda güvenli bir çıkış süreci uygulanır.
- Çıkış sürecinde aşağıdaki hususlar dikkate alınır:

  - Üniversiteye ait verilerin güvenli şekilde alınması veya aktarılması,
  - Verilerin bütünlüğünün korunması,
  - Gerekli kayıt ve logların mevzuata ve Üniversite düzenlemelerine uygun şekilde muhafaza edilmesi,
  - Kullanıcı ve yönetici hesaplarının kapatılması,
  - API, entegrasyon, servis hesabı ve benzeri erişimlerin sonlandırılması,
  - Hizmet sağlayıcı tarafından tutulan Üniversite verilerinin silinmesi,
  - Varsa veri silme işleminin gerçekleştirildiğine ilişkin kanıtların alınması,
  - Lisans, abonelik ve diğer hizmet sözleşmelerinin sonlandırılması.

- Kişisel verilerin hizmet sağlayıcı tarafından işlenmesi halinde, hizmet sonlandırma sürecinde kişisel verilerin saklanması, aktarılması ve imhasına ilişkin yükümlülükler ayrıca değerlendirilir.
- Çıkış işlemlerinin tamamlanmasının ardından gerekli kayıtlar oluşturulur ve süreç ilgili birim tarafından dokümante edilir.

6. İLGİLİ DOKÜMANLAR

- Satın Alma ve İhale Prosedürü
- Olay İhlal Prosedürü
- Bilgi Sınıflandırma ve Etiketleme Politikası
- Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası
- Erişim Kontrol Politikası

7. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	29.09.2025	İlk yayın.
001	28.09.2026	SDÜ EYS yapısına uyum sağlanması, kapsam ve sorumlulukların güncellenmesi, bulut hizmetlerinin edinim, kullanım, izleme ve çıkış süreçlerinin yeniden düzenlenmesi.