1. AMAÇ

Bu prosedürün amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında meydana gelen bilgi güvenliği, kişisel veri ve bilişim hizmetleri ile ilgili olay ve ihlallerin zamanında bildirilmesi, değerlendirilmesi, müdahale edilmesi, kayıt altına alınması, takip edilmesi ve sonuçlandırılmasına ilişkin esasları belirlemektir.

2. KAPSAM

Bu prosedür; Üniversite bünyesinde kullanılan bilgi varlıklarını, bilgi sistemlerini, bilgi ve verileri, donanım ve yazılımları, hizmetleri, dokümanları, personeli, kullanıcıları ve üçüncü tarafları kapsar.

3. TANIMLAR

- ***Olay:*** Bilgi güvenliği, kişisel veri güvenliği veya bilgi sistemlerinin gizlilik, bütünlük ya da erişilebilirliğini etkileyen veya etkileyebilecek durum.
- ***İhlal:*** Bilgi güvenliği, kişisel veri güvenliği, mevzuat, politika, prosedür veya belirlenmiş kurallara aykırılık oluşturan olay.
- ***Bilgi güvenliği olayı:*** Bilgi varlıklarının gizlilik, bütünlük veya erişilebilirliğini olumsuz etkileyen veya etkileme ihtimali bulunan olay.
- ***Kişisel veri ihlali:*** Kişisel verilerin hukuka aykırı olarak işlenmesi, erişilmesi, açıklanması, kaybolması, değiştirilmesi veya benzeri şekilde güvenliğinin ihlal edilmesi.
- ***Olay seviyesi:*** Olayın etkisine, kapsamına, kritik sistem ve hizmetlere etkisine ve müdahale gereksinimine göre belirlenen Düşük, Orta, Yüksek veya Kritik seviyelerinden biri.
- ***Olay kategorisi:*** Olayın türünü belirlemek amacıyla kullanılan SPM, MAL, ACC, DAT, DOS, DEV, CFG ve OTH kodlarından biri.
- ***Kök neden:*** Olayın meydana gelmesine yol açan temel neden veya nedenler.
- ***Küçük Olay:*** Etkisi sınırlı olan ve ilgili birim veya yetkili personel tarafından kısa sürede giderilebilen olay.
- ***Orta Olay:*** Birden fazla kullanıcıyı veya birimi etkileyen, koordinasyon veya ayrıntılı inceleme gerektiren olay.
- ***Büyük Olay:*** Kritik sistem veya hizmetleri etkileyen, geniş kapsamlı kesintiye veya ciddi bilgi güvenliği/k kişisel veri güvenliği riskine neden olan ya da üst yönetim düzeyinde değerlendirme gerektiren olay.
- ***Olay No:*** Olayın bildiriminden sonuçlandırılmasına kadar tüm kayıt ve formlarda kullanılan benzersiz takip numarası.

- ***SOME:*** Bilgi İşlem Daire Başkanlığı bünyesinde siber olaylara müdahale faaliyetlerini yürüten ekip.
- ***DİF:*** Düzeltici ve İyileştirici Faaliyet; uygunsuzluğun veya olayın temel nedenini ortadan kaldırmak ve tekrarını önlemek amacıyla yürütülen faaliyet.
- ***KVKK irtibat kişisi:*** Kişisel verilerin korunmasına ilişkin süreçlerde ilgili koordinasyon ve iletişimi yürüten görevli.
- ***Olay Bildirimi:*** Tespit edilen veya şüphelenilen olayın, değerlendirme ve müdahale sürecinin başlatılması amacıyla yetkili birimlere iletilmesi.

4. SORUMLULUKLAR

4.1. Yönetim Temsilcisi

- Olay yönetim sürecinin EYS ile uyumlu yürütülmesini gözetir.
- Büyük etkili olayları ve gerekli görülen DİF süreçlerini izler.
- Tekrarlayan veya sistemik nitelikteki olayların değerlendirilmesini ve gerekli iyileştirmelerin yapılmasını takip eder.

4.2. Bilgi İşlem Daire Başkanlığı / SOME

- Olay bildirimlerini değerlendirir, gerekli kayıtların oluşturulmasını ve olay numarasının verilmesini sağlar.
- Olayın kategorisini ve seviyesini belirler veya ilgili teknik ekiplerle birlikte belirlenmesini sağlar.
- Teknik inceleme, müdahale, kanıtların korunması ve gerekli güvenlik önlemlerini yürütür ya da koordine eder.
- Olayın etkisini, kök nedenini ve tekrarını önlemeye yönelik tedbirleri değerlendirir.
- Olay ve İhlal İşlem Formunun güncel tutulmasını, takip işlemlerinin yürütülmesini ve olayın sonuçlandırılmasını sağlar.
- Kişisel veri ihlali şüphesi bulunan olaylarda ilgili KVKK ve hukuk süreçlerinin başlatılması için gerekli koordinasyonu sağlar.

4.3. Birim Yöneticileri

- Kendi birimlerinde meydana gelen veya tespit edilen olayların gecikmeksizin bildirilmesini sağlar.
- Olayın giderilmesi için gerekli idari tedbirleri ve personel koordinasyonunu yürütür.
- Olay müdahalesi kapsamında belirlenen sorumlulukların yerine getirilmesini takip eder.
- Gerektiğinde DİF ve iyileştirme çalışmalarına katılım sağlar.

4.4. Tüm Personel ve Kullanıcılar

- Tespit ettikleri veya şüphelendikleri olayları gecikmeksizin bildirir.
- Olayın etkisini artırabilecek işlemlerden kaçınır ve yetkili personelin yönlendirmelerine uyar.
- Olayın incelenmesi ve giderilmesi için kendilerinden istenen bilgi ve desteği sağlar.

4.5. Kişisel Verilerin Korunması Sürecinde Görevli Birimler

- Kişisel verileri etkileyen veya etkileyebilecek olayları ilgili mevzuat ve kurum süreçleri çerçevesinde değerlendirir.
- Gerekli durumlarda KVKK irtibat kişisi, hukuk birimi ve ilgili yöneticilerle koordinasyon sağlar.
- Kişisel veri ihlaline ilişkin bildirim ve diğer yükümlülüklerin ilgili mevzuata uygun olarak yerine getirilmesini destekler.

5. UYGULAMA

5.1. Olayın Fark Edilmesi ve Bildirilmesi

Bilgi güvenliği, kişisel veri güvenliği veya bilgi sistemleriyle ilgili olay ya da olay şüphesi, olayı tespit eden personel, birim veya üçüncü taraf tarafından gecikmeksizin bildirilir.

Bildirim, **Olay İhlal Bildirim Formu** kullanılarak yapılır. Bildirim sürecinde olayın niteliğine göre aşağıdaki bilgiler mümkün olduğu ölçüde belirtilir:

- Olayın türü ve açıklaması,
- Olayın gerçekleştiği veya etkilediği sistem, cihaz, varlık ya da birim,
- Olayın gerçekleştiği tahmini tarih ve saat,
- Olayın tespit edildiği tarih ve saat,
- Olayın hizmetlere, sistemlere ve kullanıcılara etkisi,
- Mevcutsa ekran görüntüsü, e-posta, günlük kayıtları ve diğer kanıtlar.

Olay bildirimleri personel bildirimi, SIEM/alarm kayıtları, denetimler veya diğer tespit yöntemleri aracılığıyla da ortaya çıkabilir. Acil müdahale gerektiren olaylarda bildirim formunun tamamlanması beklenmeden Bilgi İşlem Daire Başkanlığı/SOME bilgilendirilir. Acil bildirim sonrasında gerekli kayıtlar tamamlanır.

5.2. Bildirimin Değerlendirilmesi ve Olay Kaydının Açılması

Bilgi İşlem Daire Başkanlığı/SOME tarafından bildirimin olay veya ihlal niteliği, etkilenen bilgi varlıkları ve sistemler, olayın kapsamı, bilgi güvenliği ve kişisel veri güvenliği üzerindeki etkisi ile hizmet kesintisi oluşturup oluşturmadığı değerlendirilir.

Olay veya ihlal olarak değerlendirilen bildirim için olay kaydı açılır ve benzersiz bir olay numarası oluşturulur. Olay numarası, **Olay Kodlama ve Numaralandırma Kılavuzu** doğrultusunda belirlenir.

Olayın işleme alınmasıyla birlikte **Olay ve İhlal İşlem Formu** açılır ve olayın değerlendirme, müdahale, takip ve sonuçlandırma aşamalarındaki bilgiler bu form üzerinden kayıt altına alınır. Olayın tespit yöntemi, işlemi yürüten personel ve birim ile olayın gerçekleşme, tespit ve işleme başlama tarihleri formda belirtilir.

5.3. Olayın Kategorilendirilmesi ve Seviyesinin Belirlenmesi

Olaylar, olayın türüne göre uygun kategori koduyla; etkisi, kapsamı ve müdahale gereksinimine göre Düşük, Orta, Yüksek veya Kritik seviyelerinden biriyle sınıflandırılır.

5.3.1. Olay Kategorileri

Olay kategorisi, Olay Kodlama ve Numaralandırma Kılavuzunda belirtilen aşağıdaki kodlardan seçilir:

Kod	Kategori	Açıklama
SPM	Phishing / Spam / Sosyal Mühendislik	Oltalama e-postaları, sahte mesajlar, kimlik avı bağlantıları ve aldatıcı aramalar
MAL	Zararlı Yazılım	Fidye yazılımları, virüsler, truva atları, casus yazılımlar ve benzeri zararlı yazılımlar
ACC	Yetkisiz Erişim / Hesap İhlali	Yetkisiz erişim, hesap ele geçirilmesi, parola kırma girişimleri ve benzeri olaylar
DAT	Veri İhlali / Sızıntısı	Kişisel veri sızıntısı, yanlış alıcıya veri gönderilmesi ve gizli bilgilerin ifşası
DOS	Hizmet Dışı Bırakma	Hizmetleri veya sistemleri erişilemez hâle getiren DoS/DDoS saldırıları
DEV	Donanım / Cihaz Kaybı	Kurumsal cihaz, taşınabilir bellek veya depolama ortamının kaybolması ya da çalınması

CFG	Sistem / Yapılandırma Zafiyeti	Hatalı yapılandırma, güvenlik kuralı eksikliği, güncellenmemiş sistem veya benzeri zafiyetler
OTH	Diğer / Genel Olaylar	Diğer kategorilere doğrudan girmeyen bilgi güvenliği olayları

Bir olayın birden fazla kategoriyle ilişkili olması durumunda olayın temel nedeni ve niteliği dikkate alınarak ana kategori belirlenir. Gerekli görülmesi hâlinde diğer ilgili kategoriler olay açıklamasında belirtilir.

5.3.2. Olay Seviyeleri

Olaylar etkileri ve müdahale gereksinimlerine göre **Düşük Orta, Yüksek ve Kritik** olarak sınıflandırılır.

a) Düşük Olay:

- Etkisi sınırlıdır.
- Kritik hizmet veya sistemleri etkilemez.
- Sınırlı sayıda kullanıcıyı etkiler veya etkisi kolaylıkla kontrol altına alınabilir.
- Birim veya yetkili personel tarafından giderilebilir.

b) Orta Olay:

- Birden fazla kullanıcı veya birimi etkiler.
- Hizmet veya sistem üzerinde sınırlı/orta düzeyde kesinti oluşturur.
- Birden fazla personel veya teknik ekibin koordinasyonunu gerektirir.
- Ayrıntılı inceleme veya kök neden değerlendirmesi gerektirebilir.

c) Yüksek Olay:

- Önemli bilgi varlıklarını veya kritik hizmetleri etkileyebilir.
- Birden fazla birimi veya çok sayıda kullanıcıyı etkileyebilir.
- Önemli hizmet kesintisine, ciddi güvenlik riskine veya veri kaybına yol açabilir.
- Yoğun teknik müdahale, yönetsel koordinasyon veya ilave güvenlik tedbirleri gerektirebilir

d) Kritik Olay:

- Kritik sistemlerin veya temel hizmetlerin ciddi ölçüde kesintiye uğramasına neden olur.
- Yaygın veya ağır etkili bilgi güvenliği olayı ya da kişisel veri ihlali şüphesi içerir.

- Kurumsal faaliyetlerin devamlılığını, bilgi varlıklarının güvenliğini veya mevzuattan doğan yükümlülükleri ciddi şekilde tehdit eder.
- Acil müdahale ve üst yönetim düzeyinde koordinasyon gerektirir.

Olay seviyesi belirlenirken olayın gerçekleşmiş etkisi kadar olası etkisi de dikkate alınır. İnceleme sırasında yeni bilgiler elde edilmesi durumunda olay kategorisi ve seviyesi yeniden değerlendirilerek güncellenebilir.

Olayın kategorisi ve seviyesi **Olay ve İhlal İşlem Formu** üzerinde kayıt altına alınır.

5.4. Olayın İncelenmesi ve Kök Neden Analizi

Olayın kaynağı, etkilenen varlıklar, oluş şekli ve mevcut etkileri yetkili personel tarafından incelenir.

İnceleme kapsamında aşağıdaki hususlar değerlendirilir:

- Tespit edilen durum veya güvenlik zafiyeti,
- Olayın meydana gelmesine yol açan temel neden veya nedenler,
- Etkilenen sistemler, cihazlar, bilgi varlıkları ve hizmetler,
- Olayın gizlilik, bütünlük ve erişilebilirlik üzerindeki etkileri,
- Olayın yayılma veya tekrar etme ihtimali,
- Alınması gereken kısa ve uzun vadeli tedbirler.

Kök neden henüz belirlenememişse incelemenin devam ettiği formda belirtilir. İnceleme sonucunda elde edilen bilgiler, kanıtlar ve değerlendirmeler FR-000 Olay ve İhlal İşlem Formuna kaydedilir.

5.5. Olay Müdahalesi ve Yapılan İşlemlerin Kaydı

Olayın etkisini sınırlamak, kontrol altına almak, gidermek ve tekrarını önlemek amacıyla gerekli teknik ve idari müdahaleler gerçekleştirilir.

Olayın niteliğine göre aşağıdaki işlemler uygulanabilir:

- Kullanıcı hesaplarının geçici olarak devre dışı bırakılması,
- Parola değişikliği veya erişim yetkilerinin sınırlandırılması,
- Etkilenen cihazın ağdan ayrılması,
- Zararlı yazılımın tespit edilmesi ve temizlenmesi,

- Güvenlik duvarı ve diğer güvenlik kontrollerinin uygulanması,
- Sistemlerin güvenli yapılandırmaya döndürülmesi,
- Yedekten geri yükleme veya hizmetin yeniden devreye alınması,
- İlgili kayıtların ve kanıtların korunması,
- Gerekli idari tedbirlerin alınması.

Gerçekleştirilen her işlem, sorumlusu, tarih ve saati ile işlem durumu belirtilerek "**Olay ve İhlal İşlem Formunun Yapılan Müdahale ve İşlemler**" bölümüne kaydedilir. İşlemler tamamlandığında veya devam ettiğinde ilgili durum güncellenir.

Müdahale sırasında kanıtların korunmasına, kayıtların değiştirilmemesine ve olayın etkisini artırabilecek işlemlerden kaçınılmasına dikkat edilir.

5.6. Kişisel Veri ve Gizlilik Değerlendirmesi

Olayın kişisel verileri etkilediğinin veya kişisel veri ihlali şüphesinin bulunduğunun değerlendirilmesi hâlinde, olay **Kişisel Verilerin Korunması Prosedürü** kapsamında ayrıca ele alınır.

Olay ve İhlal İşlem Formunun *KVKK ve Gizlilik Değerlendirmesi* bölümünde aşağıdaki hususlar kayıt altına alınır:

- Kişisel verilerin etkilenip etkilenmediği,
- Özel nitelikli kişisel verilerin bulunup bulunmadığı,
- Etkilenen kayıt veya kişi sayısı,
- Yasal veya KVKK bildirimi gerekip gerekmediği,
- Gizlilik veya ticari sır üzerindeki etki,
- Hukuk birimi ve/veya KVKK irtibat kişisinin bilgilendirilme durumu.

İlk değerlendirmede kesin bilgi bulunmaması hâlinde durum belirsizliğiyle birlikte kaydedilir ve inceleme sürdürülür.

Kişisel veri ihlali şüphesinin bulunması durumunda ilgili birimler gecikmeksizin bilgilendirilir. İlgili kişilere veya Kişisel Verileri Koruma Kurumuna bildirim gerekip gerekmediği, bildirimlerin zamanı ve yöntemi yürürlükteki mevzuat ile SDÜ'nün kişisel veri yönetimi süreçleri doğrultusunda değerlendirilir ve gerekli işlemler gerçekleştirilir. Kişisel veri içeren olaylara ilişkin kayıt ve kanıtlar yalnızca yetkili kişilerin erişebileceği şekilde korunur.

5.7. Uzayan Olayların Takibi

Olayın çözümünün **20 iş gününü aşması** veya olayın sonuçlandırılması için düzenli takip gerektirmesi halinde **Olay İhlal Takip Formu** kullanılır.

Olay İhlal Takip Formu üzerinde;

- yapılacak işlemler,
- sorumlular,
- hedef tarihler,
- gerçekleşme tarihleri,
- işlem durumu,
- takip notları ve sonuçları kayıt altına alınır.

Belirlenen işlemler tamamlanıncaya kadar takip kayıtları güncel tutulur. Takip gerektiren olaylarda, sonuçlandırma ve kapatma kararı verilinceye kadar Olay ve İhlal İşlem Formu ile Olay İhlal Takip Formu arasındaki ilişki korunur.

5.8. Olayın Sonuçlandırılması ve Kapatılması

Müdahale ve gerekli işlemlerin tamamlanmasının ardından olay **Olay İhlal Sonuç Formu** ile sonuçlandırılır.

Sonuç değerlendirmesinde;

- olayın kontrol altına alınıp alınmadığı,
- olayın kapatılma tarihi ve saati,
- ilave işlem gerekip gerekmediği,
- takip veya periyodik kontrol gerekip gerekmediği,
- Tekrarı önlemek için alınacak uzun vadeli tedbirler ve gerekli DİF açıklaması.

Olayın kapatılabilmesi için müdahale işlemlerinin tamamlanmış olması, olayın mevcut durumunun değerlendirilmesi ve açık kalan işlemlerin belirlenmesi gerekir.

İlave işlem veya takip gerekiyorsa bu durum formda açıkça belirtilir; gerekli işlemler tamamlanmadan olay kesin olarak kapatılmaz. Takip ihtiyacı bulunan olaylarda sorumlular ve hedef tarihler belirlenerek takip süreci yürütülür.

Olayın sonuçlandırılması, işlemi yürüten personel tarafından kayıt altına alınır. Kapatma veya onay işlemi, formda belirtilen yetkili yönetici tarafından gerçekleştirilir. İlgili personelin ve yöneticinin adı soyadı, birimi/görevi, tarih ve imza bilgileri formda belirtilir.

5.9. Düzeltici ve İyileştirici Faaliyet

Olayın tekrarlayan, sistemik veya ciddi bir zafiyetten kaynaklandığının değerlendirilmesi ya da olayın giderilmesi için mevcut kontrollerin yetersiz kalması hâlinde gerekli DİF süreci başlatılır. DİF gereksinimi değerlendirilirken olayın seviyesi, kök nedeni, etkisi, tekrar etme ihtimali ve mevcut kontrollerin yeterliliği dikkate alınır.

DİF açılması gereken durumlarda **Düzeltici ve İyileştirici Faaliyet Formu** kullanılır ve süreç **Düzeltici ve İyileştirici Faaliyet Prosedürü** doğrultusunda yürütülür. DİF başlatılması, olayın kendi kayıt ve takip sürecinin yürütülmesine engel değildir. Olay kaydı ile DİF kaydı arasında izlenebilirlik sağlanır.

5.10. İzleme, Raporlama ve İyileştirme

Olay kayıtları belirli aralıklarla değerlendirilir. Olayların türleri, seviyeleri, tekrar sıklığı, kök nedenleri, müdahale sonuçları ve kapatılma durumları analiz edilir.

Analiz sonucunda gerekli görülen durumlarda:

- Teknik ve idari kontroller gözden geçirilir.
- Sistem yapılandırmaları ve güvenlik önlemleri iyileştirilir.
- Politika, prosedür ve diğer EYS dokümanları güncellenir.
- Personel eğitimleri ve farkındalık faaliyetleri planlanır.
- Tekrarlayan olaylar için DİF başlatılır.
- Gerekli durumlarda yönetim değerlendirmesi ve ek kaynak ihtiyacı gündeme alınır.

Olay kayıtları, bilgi güvenliği yönetim sisteminin ve ilgili diğer EYS bileşenlerinin etkinliğinin değerlendirilmesinde girdi olarak kullanılır.

6. İLGİLİ DOKÜMANLAR

- Olay İhlal Bildirim Formu
- Olay ve İhlal İşlem Formu
- Olay İhlal Takip Formu
- Düzeltici ve İyileştirici Faaliyet (DİF) Formu

- Olay Kodlama ve Numaralandırma Kılavuzu
- Kişisel Verilerin Korunması Prosedürü
- Düzeltici ve İyileştirici Faaliyet Prosedürü

7. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	22.01.2020	İlk yayın.
001	27.09.2022	Sorumluluklar kısmı tüm daire başklanlıklarını kapsayacak şekilde güncellenmiştir.
002	22.01.2024	Kontrol kısmı güncellenmiştir.
003	06.12.2024	Kişisel Veri İhlal konuları eklenmiştir.
004	14.10.2026	SDÜ EYS yapısına uyum sağlanmış; olay bildirim, sınıflandırma, müdahale, takip ve sonuçlandırma süreçleri güncellenmiş; Olay ve İhlal İşlem Formu ile Olay Kodlama ve Numaralandırma Kılavuzuyla uyum sağlanmıştır.