1. AMAÇ

Bu prosedürün amacı; Süleyman Demirel Üniversitesi Daire Başkanlıkları' nın sahibi olduğu bilgi ve kişisel veri varlıklarının bilerek veya bilmeyerek, kasten veya tesadüfen 3. şahısların eline geçmesi, kısmen veya tamamen durması / tahrip edilmesi durumunda ortaya çıkan olumsuz durumları yönetmek ve olası zayıflıkları tespit ederek, zayıflıkları kullanacak tehditlerin sonuçlarını ortadan kaldırmak.

2. KAPSAM

Bu prosedür hem **ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS)** hem de **ISO 27701 Kişisel Veri Yönetim Sistemi (KVYS)** gerekliliklerini kapsar.

- Tespit edilen bilgi güvenliği ihlallerini yönetmek.
- Tespit edilen kişisel veri ihlallerini yönetmek.
- Zayıflıkların ve güvenlik açıklarının sonuçlarını yönetmek.
- İhlal veya zayıflıktan etkilenen bilgi varlıkları ve kişisel veriler üzerinde gerekli çalışmaları yürütmek.

3. SORUMLULUKLAR

Bu prosedürün uygulanmasından Süleyman Demirel Üniversitesi Daire Başkanlıkları sorumludur.
Yönetim Temsilcisi; Olay İhlal Formu ve Olay–İhlal Takip Formu süreçlerini yürütür.
KVYS Sorumlusu /İrtibat Kişisi;

- Tespit edilen olayın kişisel veri ihlali niteliğini değerlendirir.
- Kişisel veri ihlali durumunda:
  - İhlalin kapsamını belirler,
  - KVKK ya da ilgili otoriteye yapılacak bildirim gerekliliğini değerlendirir,
  - Gerekli bildirimleri 72 saat içinde koordine eder,
  - Etkilenen kişilere yapılacak bilgilendirme süreçlerini yönetir.

4. UYGULAMA

4.1.İhlalin / Zayıflığın Ortaya Çıkması / Fark Edilmesi

Bilgi güvenliği ve kişisel veri ihlal olayları kurum SOME ekibi tarafından fark edilir veya ilgili kişi ve kurumlar tarafından tespit edilerek kuruma bildirilir. Bildirime istinaden İhlal Olayı Formu / Kişisel Veri İhlal Formu düzenlenir ve Yönetim Temsilcisine iletilir. Yönetim Temsilcisi tarafından olay

- **Zayıflık** ise zayıflık kısmı,
- **Bilgi güvenliği ihlali** ise ihlal kısmı,
- **Kişisel veri ihlali şüphesi** varsa KVYS sorumlusu ile birlikte KVYS bölümünde yer alan kısım Kişisel Veri İhlal Formu doldurulur ve Kişisel Veri İhlal Formu kaydedilir.

4.2.Araştırma

İhlal olayının fark edildiği tarih ve vuku bulduğu tarihin belirlenmesi ve olayla ilişkisi olabilecek unsurların ortaya çıkarılması aşamasıdır.

Olayla ilişkili unsurlar netleştirildiğinde Olay – İhlal Formu / Kişisel Veri İhlal Formu detaylandırılır.

KVYS kapsamında araştırma sırasında aşağıdaki ek bilgiler toplanır:

- Etkilenen kişisel veri kategorileri
- Etkilenen kişi sayısı
- İhlalin gerçekleşme şekli (yetkisiz erişim, yanlış aktarım, veri kaybı vb.)
- Riskin potansiyel etkileri
- Kişilere veya kuruma yönelik oluşabilecek risklerin değerlendirilmesi

Olay – İhlal Takip Formu Some Ekibi ve Yönetim Temsilcisi tarafından gözden geçirilir. YGG toplantısında sonuçlar raporlanır; ihtiyaç duyulan eğitim, araç, yazılım, donanım vb. kaynaklar belirlenir.

4.3.Karar

Bu aşamada ihlalin ortaya çıkmasında sorumlu olan unsurlar hiçbir şüpheye yer vermeyecek şekilde ortaya konur ve karar verilir. Karar metni üç farklı içerikte hazırlanacaktır.

➢ **Personel Kaynaklı**

İhlal birim personelinden kaynaklanıyorsa disiplin yönetmeliğine göre hareket edilir. Bu durumda ihlalin kasıtlı veya bilmeyerek yapılıp yapılmadığı göz önünde bulundurulmalıdır. **Kişisel veri ihlali söz konusu ise KVYS Sorumlusu ayrıca etki analizini yapar.**

➢ **Donanım/Yazılım Kaynaklı**

İhlal bir yazılım veya donanımın hatasından kaynaklanıyor ise teknik rapor düzenlenerek yönetime sunulur. **Veri güvenliği etkilenmişse kararlı düzeltici faaliyetler belirlenir.**

➢ **3. Şahıslar**

İhlal 3. şahıslardan kaynaklanıyorsa gerekli tespitler yapılarak (IP, log kayıtları ve diğer teknik bilgiler)yönetime raporlanır. **Kişisel veri sızıntısı varsa bildirim süreci KVYS Sorumlusu tarafından yürütülür.**

4.4.Kişisel Veri İhlallerine Özgü Ek adımlar

Bir olayın kişisel veri ihlali olduğu doğrulanırsa aşağıdaki süreç zorunlu olarak işletilir:

➢ **Kişisel Veri İhlali Etki Analizi**

Aşağıdakiler değerlendirilir:

- Etkilenen veri türleri (genel / özel nitelikli)
- Veri miktarı ve kişi sayısı
- Kişilere olası etkiler (maddi, manevi zarar riski)
- İhlalin kalıcı olup olmadığı

➢ **Otorite ve Kişi Bildirimi**

- Gerekiyorsa KVKK'ya 72 saat içinde bildirim yapılır.
- Etkilenen kişilere bilgilendirme yapılır.
- İhlal Bildirim Formu KVYS dokümantasyonuna eklenir.

➢ **İyileştirme ve Önleyici Faaliyetler**

- İhlalin tekrarlanmaması için teknik ve idari tedbirler belirlenir.
- Gerekli düzeltici faaliyetler uygulanır.

5. GÜVENLİK OLAYI SINIFLANDIRMA

SEVİYE	TANIM	ÖNEM DERECESİ
1	Olay sonucunda, organizasyonun operasyonları için gerekli faaliyetlerin sürekliliği ciddi biçimde etkilenmektedir.	**Çok kritik**
2	Olay sonucunda bir uygulama veya sisteme yönelik kullanım etkilenmekte ve bu durum da organizasyonun faaliyetlerini etkilemektedir.	**Kritik**
3	Olay sadece bir kullanıcı grubunu etkilemektedir. Kesintiye uğrayan faaliyetler organizasyonun operasyonlarını etkilememektedir.	**Orta**
4	Olay sadece bir kişiyi etkilemektedir. Kesintiye uğramış faaliyetler organizasyonun operasyonlarını etkilememektedir.	**Düşük**

6. KİŞİSEL VERİ İHLALİ SINIFLANDIRMASI

SEVİYE	TANIM	KVYS AÇISINDAN DURUM
1	Özel nitelikli kişisel veri içeren ihlal	72 saat içinde otorite bildirimi zorunlu
2	Çok sayıda kişisel veri içeren ihlal (genel nitelikli)	Yüksek risk → bildirim yapılmalı
3	Az sayıda kişisel veri etkilenmiş	Risk analizi ile değerlendirme
4	Potansiyel / şüpheli kişisel veri olayı	Kayıt tutulur, izlenir

7. İLGİLİ DOKÜMANLAR

- FR-006 Olay İhlal Formu
- FR-007 Olay İhlal Takip Formu
- FR-013 Siber Olay Bildirim Formu
- FR-046 Kişisel Veri İhlal formu
- FR-047 Etkilenen Kişisel Veri İhlal Tespit formu

8. 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.