1. **AMAÇ**

 Bu prosedürün amacı; Süleyman Demirel Üniversitesi Daire Başkanlıkları’ nın sahibi olduğu bilgi 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.

1. **KAPSAM**
* Tespit edilen ihlali yönetmek.
* Zayıflıkların sonuçlarını yönetmek.
1. **SORUMLULUKLAR**

 Bu prosedürün uygulanmasından Süleyman Demirel Üniversitesi Daire Başkanlıkları

sorumludur.

1. **UYGULAMA**
	1. **İhlalin / Zayıflığın Ortaya Çıkması / Fark Edilmesi**

 Bilgi güvenliği ihlal olayları kurum SOME ekibi tarafından fark edilir veya ULAKBİM tarafından tespit edilerek kuruma bildirilir. Bildirime istinaden **İhlal Olayı Formu** düzenlenir ve Yönetim Temsilcisine iletilir. Yönetim Temsilcisi tarafından olay zayıflık ise zayıflık kısmı, ihlal ise ihlal kısmı doldurulur ve **Olay İhlal Takip Formu** kaydedilir.

* 1. **Araştırma**

 İhlal olayının fark edildiği tarih ve vuku bulduğu tarihin belirlenmesi ve olayla ilişkisi olabilecek unsurların ortaya çıkarılması aşamasıdır. İhlal olayı ile ilişkisi olabilecek unsurların belirlenmesi sonucunda **Olay İhlal Formu** düzenlenir.

 **Olay İhlal Takip Formu** **altı ayda bir** Yönetim Temsilcisi tarafından gözden geçirilir. Yönetimin Gözden Geçirme Toplantısında sonuçlar raporlanır. Yönetim, rapor çerçevesinde gerekli ihtiyaçları belirler (eğitim, araç, yazılım, donanım vs.) ve kaynakları ayırır.

* 1. **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.

* + 1. **Personel Kaynaklı**

 İhlal birim personelinden kaynaklanıyorsa disiplin yönetmeliğine göre hareket edilir. Bu durumda ihlalin kasıtlı veya bilmeyerek yapılıp yapılmadığı göz önünde bulundurulmalıdır.

* + 1. **Donanım/Yazılım Kaynaklı**

 İhlal bir yazılım veya donanımın hatasından kaynaklanıyor ise teknik rapor düzenlenerek yönetime sunulur.

* + 1. **3. Şahıslar**

 İhlal 3. şahıslardan kaynaklanıyorsa gerekli tespitler yapılarak (IP gibi) yönetime raporlanır.

1. **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** |

1. **İLGİLİ DOKÜMANLAR**
* FR-006 Olay İhlal Formu
* FR-007 Olay İhlal Takip Formu
* FR-013 Olay Bildirim Form

**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. |