1. AMAÇ

Bu prosedürün amacı bilgi varlıklarının ve ağ altyapısının güvenliğini tehdit eden olayların (Siber saldırı, DDoS, omurga kesintisi, veri sızıntısı vb.) en kısa sürede tespit edilmesi, sınıflandırılması, müdahale edilmesi, yasal bildirimlerin (BTK, USOM, KVKK) yapılması ve tekrarlanmaması için sistemin iyileştirilmesini sağlamak.

2. KAPSAM

Ufuk Üniversitesi içerisinde faaliyet gösterilen tüm çalışanları ve alanları kapsar.

3. TANIMLAR

3.1 Bilgi Güvenliği İhlal Olayı : İş operasyonlarını tehlikeye atma, bilgi güvenliğini tehdit etme olasılığı yüksek olan, gizlilik, bütünlük veya erişilebilirlik ilkelerinin ihlal edildiği istenmeyen bir dizi olaydır

3.2 Bilgi Güvenliği Olayı : Bilgi güvenliği politikalarının veya prosedürlerinin ihlal edildiğini, zayıflıkların ortaya çıktığını veya güvenlikle ilgili önlemlerin başarısız olduğunu gösteren bir olaydır

3.3 **Zayıflık (Açık):** Bir veya daha fazla tehdit tarafından istismar edilebilecek, bilgi varlığına veya bilgi güvenliği kontrolüne zarar

3.4 Kişisel Veri : Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir

3.5 Kayıt ve Bildirim Formu : İhlal olayını fark eden personelin durumu detaylarıyla (tarih, saat, olay) belgeleyerek BGYS sorumlusuna ilettiği dokümandır

3.6 **USOM :** Ulusal Siber Olaylara Müdahale Merkezi (BTK'ya bağlı, siber olayların ulusal koordinasyon merkezi)

3.7 **SOME (Siber Olaylara Müdahale Ekibi):** Bir kurum içinde siber olaylara müdahale etmekle görevli, teknik ve idari karar vericilerden oluşan ekiptir.

3.8 Risk Kabul Kriterleri : Risklerin değerlendirilmesinde baz alınan, kurumun göze alabileceği maksimum risk seviyesi

3.9 Tehdit : Bilgi sistemine veya kuruluşa zarar verme potansiyeli olan, istenmeyen bir olayın (siber saldırı, doğal afet, kullanıcı hatası) meydana gelme ihtimali

3.10 Zafiyet (Açıklık): Bir varlığın veya kontrolün, tehdit veya tehditler tarafından istismar edilebilecek zayıf yönü

4. UYGULAMA

4.1 İhlalin / Zayıflığın Ortaya Çıkması / Fark Edilmesi

İhlal olayını fark eden personel olayla ilgili olarak ivedilikle Bilgi İşlem Daire Başkanlığına veya BGYS Temsilcisi haberdar eder ve İhlal Olayı Formu düzenler ve BGYS Temsilcisine iletir.
BGYS Temsilcisi olay zayıflık ise zayıflık kısmı ihlal ise ihlal kısmı doldurulur ve Olay İhlal Takip Çizelgesine kaydedilir.

4.2 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.

HAZIRLAYAN <HAZ_POZ_TAN>	KONTROL_EDEN <KONT_POZ_TAN>	ONAYLAYAN <SON_ONAY_POZ_TAN>

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

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.

- **İhlal Personel:** İhlal firmamız personelinden kaynaklanıyorsa disiplin yönetmeliğine göre hareket edilir. Bu durumda ihlalin kasıtlı veya bilmeyerek yapılıp yapılmadığı göz önünde bulundurulmalıdır.
- **İhlal Donanım /Yazılım:** İhlal bir yazılım veya donanımın hatasından kaynaklanıyor ise teknik rapor düzenlenerek yönetime sunulur.
- **İhlal 3. Şahıslar:** İhlal 3. şahıslardan kaynaklanıyorsa gerekli tespitlerin yapılarak (ip no gibi) yönetime raporlanır.

4.4 Güvenlik Olayı Sınıflandırma

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

5. İLGİLİ DOKÜMANLAR

5.1 Olay İhlal Formu
5.2 Olay İhlal Çizelgesi
5.3 Disiplin Prosedürü
5.4 Uygunsuzluk Yönetimi Düzeltici ve İyileştirici Faaliyet Prosedürü
5.5 İyileştirici Faaliyetler Prosedürü

HAZIRLAYAN <HAZ_POZ_TAN>	KONTROL_EDEN <KONT_POZ_TAN>	ONAYLAYAN <SON_ONAY_POZ_TAN>