	OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI		
Doküman No: PLT.31	**Yayın Tarihi:** 25.04.2022	**Revizyon Tarihi:** -	**Revizyon No:** -

1. AMAÇ

Bu politikanın amacı Muğla Sıtkı Koçman Üniversitesi'nin bilgi güvenliği olay ihlal süreçlerini belirlemektir.

2. KAPSAM

Bu politika, Muğla Sıtkı Koçman Üniversitesi'ne bilgi varlıklarını kullanmakta olan tüm kullanıcılar için geçerlidir.

3. KISALTMALAR

Bu prosedürde geçen;

3.1. MSKÜ: Muğla Sıtkı Koçman Üniversitesi'ni ifade eder.

4. TANIMLAR

4.1. DDOS Atağı (Distributed Denial of Service Attack): Çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşur, bunlar genellikle bir veya birden fazla web sunucusudur. Bu sistemler saldırganlar tarafından çeşitli yöntemler kullanılarak bağdaştırılır.

5. SORUMLULUKLAR

Bu politika ile ilgili gereklerin uygulanmasından dahili veya harici olarak yararlanan tüm kullanıcılar sorumludur.

6. UYGULAMA

a) Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.

b) Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

c) Bilgi güvenliği ihlali oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.

d) Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır. İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

e) Güvenlik ihlaline neden olan kullanıcılar için resmi bir disiplin sürecine başvurulmalıdır.

f) Tüm kullanıcılar bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan Bilgi İşlem Daire Başkanlığına mümkün olan en kısa sürede rapor etmelidir.

Hazırlayan Bilgi Güvenliği Ekibi	Kontrol Eden Bilgi İşlem Daire Başkanlığı	Onaylayan Rektör Yardımcısı

g) Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, DDOS atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlalleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınmalıdır.
h) Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması, uygulanması ve ilgili otoritelere raporlanması konuları göz önüne alınır.
i) İç problem analizi, adli incelemeler veya üretici kurumdan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanmalıdır.
j) Aynı olayın tekrar etmesini önlemek veya yüksek etkili olayların oluşmasını engellemek için bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ve tecrübe ile yeni kontrollerin oluşturulması gerekmektedir.

6.1. Yaptırım

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri, tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

7. İLGİLİ DOKÜMANLAR

-

Hazırlayan	Kontrol Eden	Onaylayan
Bilgi Güvenliği Ekibi	Bilgi İşlem Daire Başkanlığı	Rektör Yardımcısı