1. AMAÇ: Bu politika; Ankara Medipol Üniversitesi kapsamında, bilginin gizlilik, bütünlük sürekliliğini sağlamak, risk yönetimini güvence altına almak, bilgi güvenliği yönetimi süreç performansını ölçmek ve bilgi güvenliği ile ilgili konularda üçüncü taraflarla olan ilişkilerin düzenlenmesini amacı ile hazırlanmıştır.

2. KAPSAM: Bu politikanın kapsamı tüm organizasyon ve bilgi varlıklarını kapsamaktadır.

3. SORUMLULUK

3.1. Bilgi Teknolojileri Daire Başkanlığı: Bilgi Güvenliği Politikasının kurum ihtiyaçlarını karşılar nitelikte bulunmasından ve politikanın uygulanması için gerekli destek ve gözetimin sağlanmasından, gerekli durumlarda gözden geçirilmesinden sorumludur.

3.2. Bilgi Güvenliği Yöneticisi: Kalite Koordinatörü, Bilgi Teknolojileri Koordinatörü, İnsan Kaynakları Koordinatörü ve Bilgi Güvenliği Koordinatöründen oluşan komisyondur. Kurumun Bilgi Güvenlik ile ilgili kararlarının alınmasından ve uygulanmasından sorumludur. 3 Ayda bir toplanır.

3.3. Bilgi Güvenliği Komisyonu: Kalite Komisyonu Koordinatörü, Bilgi Güvenlik Koordinatörü, İnsan Kaynakları ve Planlama Koordinatörlüğü, İdari ve Mali İşler Koordinatörlüğü ve Bilgi Teknoloji Koordinatörlüğü oluşan komisyondur. Kurumun Bilgi Güvenlik ile ilgili kararlarının alınmasından ve uygulanmasından sorumludur. 3 Ayda bir toplanır.

3.4. Tüm Personel: Bilgi Güvenliği Politikasının ve BG Komisyonu'nun aldığı kararların görev alanlarının gerektirdiği biçimde yerine getirmekten sorumludur.

4. UYGULAMA

4.1. Bilgi Güvenliği Politikası

- Ankara Medipol Üniversitesi bünyesinde bilginin gizliliğini, erişebilirliğini, bütünlüğünü ve sürekliliğini sağlamak politikanın esasını oluşturur.
  - **Gizlilik: Önem taşıyan bilgilere yetkisiz erişimlerin önlenmesi,**
  - **Bütünlük: Bilginin doğruluk ve bütünlüğünün sağlandığının gösterilmesi,**
  - **Erişebilirlik: Yetkisi olanların gerektiği hallerde bilgiye ulaşılabilirliğinin gösterilmesidir.**

Ankara Medipol Üniversitesi BİLGİ TEKNOLOJİLERİ DAİRE BAŞKANLIĞI Tarafından Yürütülen Bilgi İşlem Faaliyetlerinin Bilgi Güvenliği Hizmetleri kapsamında;

- Bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek ve uygulamak.
- Yasal ve ilgili mevzuat gereklerini yerine getirmek, anlaşmalardan doğan yükümlülüklerini karşılamak ve iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.
- Sadece elektronik ortam da tutulan verilerin değil; yazılı, basılı, sözlü ve benzeri ortam da bulunan tüm verilerin güvenliği ile ilgilenmek.
- Bilgi Güvenliğindeki gerçekte var olan veya şüphe uyandıran tüm açıkların, BGYS Ekibine rapor etmek ve BGYS Yöneticisi tarafından soruşturulmasını sağlamak,
- Bilgi Güvenliği konusunda periyodik olarak değerlendirmeler yaparak mevcut riskleri tespit etmek. Değerlendirmeler sonucunda, aksiyon planlarını gözden geçirmek ve takibini yapmak,
- İş sürekliliğinde bilgi güvenliği tehditlerinin etkisini azaltmak, sürekliliğe katkıda bulunmak ve test etmek,
- Sözleşmelerden doğabilecek her türlü anlaşmazlık ve çıkar çatışmasını engellemek,
- Bilgiye erişebilirlik ve bilgi sistemleri için iş gereksinimlerini karşılamaktır.
- Bilgi güvenliği yönetimi eğitimlerini tüm personele vererek bilinçlendirmeyi sağlamak.
- BT güvenliği fiziksel erişim güvenliğinden siber güvenlik seviyesine kadar bütüncül olarak ele almak.
- ISO 27001 standartlarına uygun bir güvenlik seviyesine ulaşmak hedefi ile çalışmak.
- Kullanılan güvenlik yazılım ve donanımları sürekli kontrol altında tutmak. Kritik sistemlerin 24 saat izlenmesini sağlamak.

5. İLGİLİ SÜREÇLER

5.1. BT Yetkilendirme Süreci,

5.2. BT Erişim Yönetimi Süreci,

5.3. BT Güvenlik Olay Yönetimi Süreci

6. YAPTIRIM

Bu politikaya ve ilgili süreçlere uygun olarak çalışmayan tüm personel hakkında **Disiplin Prosedürü** hükümleri uygulanır.

7. İLGİLİ DOKÜMANLAR

7.1. Disiplin Prosedürü