AMAÇ

Bu politika; MEDİPOL Eğitim ve Sağlık Grubu'nda bilginin gizlilik, erişilebilirlik, bütünlük ve sürekliliğini sağlamak, temel bilgi güvenliği prensiplerini kurum stratejisine uyumlu olarak tanımlamak ve bu prensiplere üst yönetimin verdiği desteği ifade etmek amacı ile hazırlanmıştır.

SORUMLULUK

BT Üst Yönetim

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

Bilgi Güvenliği Yöneticisi

Bilgi Güvenliği Yöneticisi, Bilgi Güvenliği Politikasının kurum ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından ve Bilgi Güvenliği Komitesi'ni yönetmekten sorumludur.

Bilgi Güvenliği Komitesi

Genel Müdür, Medikal Direktör, Rektör, Bilgi Güvenlik Koordinatörü, İnsan Kaynakları Direktörü ve İdari İşler Direktöründen oluşan kuruldur. Kurumun Bilgi Güvenlik ile ilgili kararlarının alınmasından ve uygulanmasından sorumludur. 3 Ayda bir toplanır.

Tüm Personel

Bilgi Güvenliği Politikasının ve BG Kurulu'nın aldığı kararların görev alanlarının gerektirdiği biçimde yerine getirmekten sorumludur.

KAPSAM

Bu politikanın kapsamı tüm organizasyon ve bilgi varlıklarıdır.

UYGULAMA

Bilgi Güvenliği Politikası

- Medipol Grup bünyesinde bilginin gizliliğini, erişebilirliğini, bütünlüğünü ve sürekliliğini sağlamak politikanın esasını oluşturur.
- 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.
- İş sürekliliğinde bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak.
- Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmak.
- Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek.
- Bilgi güvenliği yönetimi eğitimlerini tüm personele vererek bilinçlendirmeyi sağlamak.
- Yürütülen tüm faaliyetlerde; bilgi güvenliğini, risk yönetimi çerçevesinde ele alarak risklerin ortadan kaldırılmasını hedeflemek.
- 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 izlenmesi.
- Merkezi ve dağıtık yapılarda gerekli güvenlik güncellemelerinin düzenli olarak yapılması.
- Tüm BT alanlarına girişlerin kontrollü olarak yapılması ve kayıt altına alınması.

İLGİLİ SÜREÇLER

BT yetkilendirme süreci, BT erişim yönetimi süreci, BT güvenlik olay yönetimi süreci

YAPTIRIM

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