1. GİRİŞ VE AMAÇ

Phitech, makina öğrenmesi, yapay zeka tabanlı çözümleri ve biyoteknoloji alanlarında hizmet vermektedir. Bu alanlarda yüksek güvenlik gerektiren anonimleştirilmiş genetik, algoritmalar, prototipler, AR-GE çıktıları ve tıbbi araştırma verileri barındırılmaktadır.
Bu politikanın amacı, ISO/IEC 27001:2022 standardına uygun olarak kurumun **bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini** güvence altına almaktır. Ayrıca, paydaşlarımıza bilgi güvenliği taahhüdümüzü beyan etmek ve çalışanlarımız için yol gösterici ilkeleri tanımlamak da bu politikanın hedefleri arasındadır.

---

2. KAPSAM

Bu politika;

- Phitech'in merkez ofisi ve Ar-Ge laboratuvarları,
- Tüm dijital altyapı (sunucular, veritabanları, web platformları, IoT cihazları, yazılım kaynak kodları),
- Çalışanlar, stajyerler, danışmanlar, taşeronlar, üçüncü taraf hizmet sağlayıcılar,
- Tıbbi veri işleme süreçleri, yapay zeka modelleri ve analiz altyapılarını kapsamaktadır.

---

3. POLİTİKA İLKELERİ

3.1. Gizlilik

- Hasta verileri, klinik çalışma çıktıları ve AR-GE projeleri yalnızca yetkili kullanıcılar tarafından erişilebilir olacak şekilde şifreleme, rol bazlı erişim yöntemleriyle korunur.
- Üçüncü taraflarla veri paylaşımı sadece sözleşmesel düzenlemeler ve gizlilik anlaşmaları çerçevesinde yapılır.

3.2. Bütünlük

- Verilerin tahrif edilmesini, izinsiz değiştirilmesini önlemek için donanım hatalarından kaynaklı bozulmaları engellemek. İzinsiz erişimleri engellemek için izin kontrol sistemleri kontrolleri (örn. hash algoritmaları) uygulanır.

- Yazılım geliştirme süreçlerinde versiyon kontrol sistemleri ve değişiklik denetimleri kullanılır.

3.3. Erişilebilirlik

- Kritik sistemlerin 7/24 erişilebilirliğini sağlamak için yedekleme, UPS ve acil durum planı uygulama sistemleri uygulanır.

- Web tabanlı yazılımlar ve mobil uygulamalar için uptime oranları %99'in üzerinde tutulur.

3.4. Yasal ve Regülasyon Uyumu

- Türkiye'de **KVKK**, Avrupa Birliği'nde **GDPR** ve diğer uluslararası regülasyonlara tam uyum sağlanır.

- Dış kaynaklı doküman takip sisteminde ilgili mevzuatların takibinin yapılması ve uygulanması

3.5. Risk Temelli Yaklaşım

- Bilgi güvenliği risk değerlendirmesi yılda en az bir defa gerçekleştirilir.

- Riskler, etki ve olasılık düzeylerine göre sınıflandırılarak uygun kontrollerle azaltılır.

3.6. Olay Yönetimi ve Bildirim

- Herhangi bir bilgi güvenliği olayı (veri sızıntısı, kötü amaçlı yazılım, yetkisiz erişim) derhal raporlanmalı ve en fazla 72 saat içinde ilgili mercilere bildirilmelidir (KVKK kapsamında).

- Olaylar sonrasında kök neden analizi yapılır ve düzeltici/önleyici faaliyetler başlatılır.

3.7. İnsan Kaynakları ve Farkındalık

- Tüm personel işe başlamadan önce bilgi güvenliği eğitimi alır.

- Bilgi güvenliği farkındalık kampanyaları (phishing simülasyonları, e-posta güvenliği, güçlü parola kullanımı) düzenli olarak yürütülür.

3.8. Fiziksel ve Çevresel Güvenlik

- Sunucu odaları ve hassas veri içeren fiziksel alanlar giriş kontrol sistemleri ile korunur.
- Teknokent güvenliğinin sorumluluğunda ve erişim logları düzenli olarak kontrol edilir.

3.9. Tedarikçi ve Dış Kaynaklı Hizmet Güvenliği

- Üçüncü taraf firmalarla yapılan hizmet sözleşmelerinde bilgi güvenliği şartları yer alır.
- Tedarikçiler yıllık olarak performans ve güvenlik kriterlerine göre değerlendirilir.

3.10. İş Sürekliliği ve Felaket Kurtarma

- Elektrik kesintisi, siber saldırı, donanım arızası gibi durumlara karşı kriz planı ve kurtarma senaryoları geliştirilmiştir.
- Kritik sistemler için günlük yedeklemeler alınmakta ve başka lokasyonlarda güvenli şekilde saklanmaktadır.

---

4. UYGULAMA, DENETİM VE İYİLEŞTİRME

- Bilgi Güvenliği Yönetim Sistemi performansı yılda bir kez gözden geçirilir.
- İç denetimler ve yönetim gözden geçirme toplantıları yoluyla sistemin etkinliği takip edilir.
- BGYS sürekli iyileştirme döngüsü (Planla-Uygula-Kontrol Et-Önlem Al, PDCA) ile işletilir.

---

5. YETKİ VE SORUMLULUKLAR

Rol	Sorumluluklar
Genel Müdür	Politikanın onaylanması ve kaynak tahsisi
Bilgi Güvenliği Yöneticisi	BGYS'nin kurulması, sürdürülmesi, izlenmesi ve iyileştirilmesi
Tüm Çalışanlar	Politika ve ilgili prosedürlere uyum, olay bildirimi
BT Ekibi	Sistem güvenliği, ağ güvenliği, yedekleme, güncelleme

---