

Bilgi Güvenliği Deklarasyonu

Sürüm 1.0

Yürürlük	Yönetim Kurulu onayıyla yürürlüğe girer; yılda en az bir kez gözden geçirilir
Sürüm	1.0
Tarih	29 Eylül 2026
Hazırlayan/Düzenleyen	Prof. Dr. Gökmen Zararsız
Onaylayan	Yönetim Kurulu, Hematainer Biyoteknoloji ve Sağlık Ürünleri A.Ş. Kayseri, Türkiye
Değişiklik Gerekçesi	İlk sürüm

1. Giriş

MAS® ürün ailesi, analiz hizmetleri, araştırma projeleri ve OmegaTree kapsamında oluşan bilgilerin gizliliğinin, bütünlüğünün ve ihtiyaç duyulduğunda erişilebilirliğinin korunması, Hematainer yönetimi tarafından kurumsal bir sorumluluk olarak benimsenir. Bu deklarasyonda, çalışanların ve iş ortaklarının uyması gereken genel güvenlik ilkeleri ile yönetimin iyileştirme taahhüdü açıklanır.

2. Kapsam ve Varlıklar

Kapsam; fiziksel ve dijital kayıtlar, biyolojik örnekler ve örnek kimlikleri, metabolomik ve lipidomik ham veriler, analiz sonuçları, biyoinformatik kod ve modeller, OmegaTree geliştirme verileri, fikri mülkiyet, teknik dosyalar, tedarikçi ve müşteri bilgileri ile bunları işleyen cihaz, yazılım ve hizmetlerden oluşur. İlkeler, görev ve konumdan bağımsız olarak çalışanlara, araştırmacılara, stajyerlere, danışmanlara ve erişim verilen hizmet sağlayıcılara uygulanır.

3. Yönetim Taahhütleri

- ✓ Bilgi varlıkları sınıflandırılır; özellikle sağlık ve genetik veriler, kimlik bağlantıları, yayımlanmamış araştırmalar ve ticari sırlar için risk temelli koruma uygulanır.
- ✓ Erişimler görev gereğine göre verilir, düzenli olarak gözden geçirilir ve görev değişikliğinde ya da ayrılıştan kaldırılır. Paylaşımlarda ve sistem erişimlerinde kimlik doğrulama, kayıt ve uygun teknik güvenlik kontrolleri risk düzeyine göre uygulanır.
- ✓ Veri aktarımı, saklama, yedekleme ve geri yükleme, cihaz güvenliği ve fiziksel erişim süreçleri tanımlanır; hizmet sağlayıcıların güvenlik ve gizlilik yükümlülükleri sözleşmelerde belirlenir.
- ✓ Araştırma verileri ile kişiyi tanımlayan bilgiler mümkün olduğunca birbirinden ayrılır; proje amacı dışında kullanım ile yetkisiz kopyalama veya paylaşım önlenir.
- ✓ Bilgi güvenliği olayları hızla bildirilir; olayın etkisi sınırlandırılır, kayıt altına alınır, kök nedeni değerlendirilir ve gerekli düzeltici adımlar izlenir. Kişisel veri ihlallerinde ilgili bildirim yükümlülükleri ayrıca değerlendirilir.
- ✓ İş sürekliliği gereksinimleri belirlenir; kritik verilere ve hizmetlere ilişkin yedekleme ve geri dönüş düzenlemeleri sınırlanır.

4. Roller ve Davranış Kuralları

Yönetim, güvenlik hedeflerinden ve kaynaklarından sorumludur; süreç sahipleri kendi varlıklarını ve risklerini izler. Bilgiye erişen herkes; bilgiyi yetkisi dâhilinde kullanmak, kimlik bilgilerini korumak, şüpheli e-posta, kayıp cihaz, yanlış alıcıya iletim veya yetkisiz erişim gibi olayları gecikmeden bildirmek ve gizlilik yükümlülüğüne uymakla sorumludur. Eğitim ve farkındalık faaliyetleri, görevlerin riskine uygun olarak yürütülür.

5. Uyum ve Gözden Geçirme

6698 sayılı Kişisel Verilerin Korunması Kanunu, araştırma etiği, sözleşmeler ile ürün ve laboratuvar faaliyetlerine uygulanabilir düzenlemeler dikkate alınır. Riskler, olaylar, teknoloji ve iş ortaklıkları değiştiğinde kontroller güncellenir. Uygulama durumu ve iyileştirme ihtiyaçları, yönetim tarafından en az yılda bir kez değerlendirilir.

Güvenlik ve gizlilik bildirimleri için iletişim: info@hematainer.com. Olayın niteliğine göre Hematainer ekibi tarafından güvenli bir iletişim kanalı belirlenir.

Onay tarihi: Eylül 2026

Bu doküman Hematainer Biyoteknoloji ve Saęlık Ürünleri A.Ş. kurucu ortaklarının tümü tarafından imzalanmıřtır.

Prof. Dr. Mehmet Doęan



Prof. Dr. Halef Okan Doęan



Prof. Dr. Gökmen Zararsız

