

Doküman: Airisto Bilgi Güvenliği Politikası

Belge Adı: Airisto - Bilgi Güvenliği Politikası

Sürüm: 1.0

Son Güncelleme Tarihi: 05.09.2025

1. Amaç ve Kapsam

1.1. Politikanın Amacı:

Bu Bilgi Güvenliği Politikası'nın ("Politika") temel amacı, Airisto'nun sahip olduğu, işlediği ve sorumlu olduğu tüm bilgi varlıklarını iç ve dış tehditlere karşı korumak; hizmetlerimizin, kullanıcı verilerinin ve operasyonel süreçlerimizin **Gizlilik, Bütünlük ve Erişilebilirlik** ilkelerini en üst düzeyde sağlamaktır. Bu politika, bilgi güvenliği risklerini yönetmek, yasal ve düzenleyici gerekliliklere uymak ve kullanıcılarımıza güvenilir bir platform sunmak için oluşturulmuş temel çerçeveyi tanımlar.

1.2. Kapsam:

Bu politika, Airisto bünyesindeki tüm çalışanları, yöneticileri, iş ortaklarını ve alt yüklenicileri kapsar. Ayrıca, Platformumuz tarafından işlenen tüm verileri (kullanıcı kişisel verileri, analiz içerikleri, finansal veriler, operasyonel veriler) ve bu verileri işleyen tüm teknolojik altyapıyı (sunucular, ağlar, yazılımlar, veritabanları) kapsar.

2. Bilgi Güvenliği Yönetim Çerçevesi

Airisto, bilgi güvenliğini tesadüfi önlemlerle değil, ISO/IEC 27001 gibi uluslararası kabul görmüş standartları referans alan, proaktif ve bütüncül bir yönetim anlayışıyla ele alır.

2.1. Temel İlkeler:

- Gizlilik (Confidentiality):** Bilgiye yalnızca yetkili kişiler tarafından erişilebilmesini sağlamak. Platforma analiz için yüklenen içeriklerin mutlak gizliliği bu ilkenin temelidir.
- Bütünlük (Integrity):** Bilginin yetkisiz değiştirmelere, bozulmalara veya silinmelere karşı korunarak doğruluğunu ve tutarlılığını sürdürmesini sağlamak.
- Erişilebilirlik (Availability):** Yetkili kullanıcıların, ihtiyaç duydukları anda bilgiye ve ilgili hizmetlere kesintisiz bir şekilde erişebilmesini sağlamak.

2.2. Sorumluluklar:

- **Yönetim:** Bilgi güvenliği politikalarının oluşturulmasından, kaynak ayrılmasından ve denetlenmesinden üst yönetim sorumludur.
- **Tüm Çalışanlar:** Tüm çalışanlar, bu politikada belirtilen kurallara uymakla, güvenlik farkındalığına sahip olmakla ve olası güvenlik ihlallerini bildirmekle yükümlüdür.

3. Teknik Güvenlik Kontrolleri ve Önlemleri

Platformumuzun ve verilerinizin güvenliğini sağlamak için uyguladığımız temel teknik kontroller şunlardır:

3.1. Ağ ve Altyapı Güvenliği:

- **Güvenlik Duvarları (Firewalls):** Ağ trafiğini kontrol etmek ve yetkisiz erişimleri engellemek için yeni nesil güvenlik duvarları kullanılır.
- **Saldırı Tespit ve Önleme Sistemleri (IDS/IPS):** Ağ üzerindeki şüpheli aktiviteleri ve saldırı girişimlerini anlık olarak izleyen ve otomatik olarak engelleyen sistemler aktiftir.
- **Güvenli Konfigürasyon:** Tüm sunucular, ağ cihazları ve yazılımlar, gereksiz port ve servislerin kapatıldığı, "güvenli yapılandırma" (hardening) prensiplerine göre yapılandırılır.

3.2. Veri Şifreleme:

- **Aktarım Sırasında Şifreleme (Encryption in Transit):** Kullanıcı cihazı ile sunucularımız arasındaki tüm veri akışı, endüstri standardı olan SSL/TLS protokolleri ile güçlü bir şekilde şifrelenir.
- **Depolanırken Şifreleme (Encryption at Rest):** Veritabanlarımızda saklanan tüm kullanıcı kişisel verileri, en güncel kriptografik algoritmalar kullanılarak şifrelenmiş olarak muhafaza edilir.
- **Analiz İçeriklerinin İmhası:** Analiz için yüklenen metin içerikleri, analiz süreci tamamlandıktan hemen sonra geri döndürülemez şekilde silindiği için, bu geçici verilerin uzun süreli depolanması ve buna bağlı riskler ortadan kaldırılmıştır.

3.3. Erişim Kontrolü ve Kimlik Doğrulama:

- **En Az Ayrıcalık Prensibi (Principle of Least Privilege):** Çalışanların sistemlere ve verilere erişimi, yalnızca görevlerini yerine getirmeleri için mutlak surette gerekli olan minimum yetkilerle sınırlandırılmıştır.

- **Güçlü Parola Politikaları:** Tüm kullanıcı ve yönetici hesapları için karmaşık parola standartları zorunlu tutulur.
- **Çok Faktörlü Kimlik Doğrulama (MFA):** Hassas sistemlere ve yönetici panellerine erişim, ek bir güvenlik katmanı olarak Çok Faktörlü Kimlik Doğrulama ile korunur.

3.4. Yazılım Geliştirme Güvenliği (DevSecOps):

- **Güvenli Kodlama Pratikleri:** Yazılım geliştirme süreçlerimizin her aşamasında, OWASP gibi uluslararası standartlara uygun güvenli kodlama pratikleri uygulanır.
- **Kod Analizi ve Zafiyet Taramaları:** Geliştirilen kodlar, yayınlanmadan önce statik ve dinamik kod analizi (SAST/DAST) araçlarıyla güvenlik zafiyetlerine karşı taranır.

4. İdari ve Fiziksel Güvenlik Kontrolleri

- **Güvenlik Farkındalığı Eğitimi:** Tüm çalışanlar, ortalama (phishing) saldırıları, sosyal mühendislik ve güvenli veri kullanımı gibi konularda düzenli olarak bilgilendirilir ve eğitilir.
- **Olay Yönetimi ve Müdahale Planı:** Olası bir güvenlik ihlali (veri sızıntısı, hizmet kesintisi vb.) durumunda atılacak adımları, sorumlu kişileri ve iletişim süreçlerini tanımlayan bir "Olay Müdahale Planı" mevcuttur.
- **Fiziksel Güvenlik:** Hizmetlerimizin barındırıldığı veri merkezleri, biyometrik erişim kontrolleri, 7/24 güvenlik personeli, CCTV izleme ve çevresel kontrol sistemleri gibi en üst düzey fiziksel güvenlik önlemlerine sahiptir.

5. Politikanın Gözden Geçirilmesi ve Güncellenmesi

Bu Bilgi Güvenliği Politikası, teknolojik gelişmeler, yeni ortaya çıkan tehditler ve yasal düzenlemeler doğrultusunda yılda en az bir kez veya gerekli görüldüğünde gözden geçirilir ve güncellenir.