NebulaByte AI Consultation - Deployment and Security Considerations

Date: October 9, 2025

Participants: Dr. Sarah Chen (Lead AI Architect), Michael Rodriguez (Software Engineer), Lisa Wong (Product Manager)

Deployment Strategy:

The multi-agent system will be deployed using containerized microservices:

1. Backend Services: - FastAPI application container - FAISS vector store persistence - Redis for caching and session management

2. Frontend: - Static HTML/CSS/JS served via CDN - WebSocket connection for real-time updates

3. Hosting Platforms: - Primary: Hugging Face Spaces - Backup: Render.com - Local development: Docker Compose

Security Measures:

1. API Security: - Rate limiting per IP and user - API key authentication for external services - Input validation and sanitization

2. File Upload Security: - Maximum file size: 10MB - File type validation (PDF only) - Content scanning for malicious code - Temporary storage with automatic cleanup

3. Data Privacy: - No PII storage in logs - Encrypted data transmission (HTTPS) - GDPR-compliant data handling

Monitoring and Logging: - Real-time system health monitoring - Performance metrics collection - Error tracking and alerting - Audit logs for compliance