ARTEFACT 3

Risk, Security & Governance Model

Key Risks and Mitigation

Risk Area	Description	Mitigation
Model Overreach	AI generating misleading enhancements	Human custom color hint control
Data Integrity	Loss of original data fidelity	Structured saving of original + mask + output
Reproducibility	Inability to retrace results	.npy export for training and reprocessing
Scalability	Prototype Stagnation	Modular PyTorch-based architecture

---

Governance Structure

- Clear separation between model inference and user input
- Reproducible output storage standards
- Planned enterprise package (.exe distribution)
- Roadmap for batch processing and extended features

Public Trust & Ethical AI

Although internal-facing, the platform was designed to ensure:

- Human oversight over AI outputs
- Transparent differentiation between original and generated imagery
- Data integrity

This protects institutional credibility when AI-enhanced outputs are used in analysis.