Responsible AI Audit Report

Case: Verification of Misleading Internship Platform Claiming NSDC Partnership

Author: Suganya P (AI Product & Governance Professional)

Date: October 2025

1. Audit Purpose

This audit was conducted after encountering an internship platform that appeared credible and claimed affiliation with the National Skill Development Corporation (NSDC). The goal was to verify authenticity and assess potential risks to users, particularly students and professionals in AI.

2. Context

The platform offered instant offer letters, professional design, and government-like branding. However, discrepancies in listed partners and community reports raised suspicions, prompting this audit.

3. Audit Methodology

The S-RAIEF Framework (Security, Responsibility, Accountability, Integrity, Explainability, Fairness) was used to structure the verification process. Steps included checking NSDC portal, reviewing social platforms, validating evidence, performing digital forensics, and raising awareness.

4. Key Observations

- Unauthorized use of NSDC logos to simulate authenticity
- Potential data privacy risks
- UI design mimicking official government interfaces
- Lack of transparency and contact details
- Risk of social engineering attacks

5. Responsible AI Audit Analysis

Governance Impact: Breach of Transparency and Integrity principles under OECD AI Principles. Violates Accountability under NIST AI RMF (2023).
Ethical concern: misuse of trust and misrepresentation of AI credibility.

6. Preventive Recommendations

For Users: Verify claims on official portals, review social feedback, avoid sharing personal data.
For Platforms: Implement governance validation, transparency logs, and ethical branding.
For Policymakers: Create centralized verification for AI training partners, mandate Responsible AI audits.

7. Governance Outcome

The case was flagged and shared publicly to prevent misinformation. No data compromise detected. Serves as proof of ethical vigilance in Responsible AI practice.

8. Lessons Learned

Security: Always scan systems post-interaction.
Responsibility: Verify before sharing.
Accountability: Report false information.
Integrity: Maintain authenticity.
Explainability: Share findings clearly.
Fairness: Help others gain awareness.

9. Conclusion

AI Governance begins with human responsibility. Verifying before trusting reflects the core of Responsible AI. This audit highlights ethical awareness and integrity in practice.

10. Author’s Reflection

“True AI Governance is not only about regulating systems — it’s about guiding human choices that shape the AI world. Awareness is our first defense, and integrity is our lasting strength.” – Suganya P, 2025