Engineering Ethics Report Template

Project Title: AI-Driven Budgeting Suite: Intelligent Forecasting and Dynamic Budget Management

Team Members:
Ryan Ellis
Varshini Muniswaran
Rounak Sharma
Ansh Hemang Dani
Maaz Naqvi

Identified Ethical Issues

1. **Issue:** The use of your company's data to populate the AI with information to then make predictions for you in the future, but also for others in the future.
2. **Category:** Data Privacy and Security
3. **Potential Consequences:** Potential for very sensitive data to be leaked to the public or to competitors.
4. **Stakeholders Affected:** The owner of the company, employees, investors, and business partners.
5. **Impact:** I would classify this as a medium to high risk. There is always potential that information gets leaked to a source that doesn't know what to make of it, but the info would still be out in the world at that point, causing a medium risk. With that said, it could be maliciously obtained by a competitor to see where you stand financially and potentially how they can harm your business, causing a high risk.
6. **Relevant Professional Codes:**

ACM Code of Ethics

- 1.6 Respect privacy: Professionals must only use personal or organizational data for legitimate ends, and with consent. Using company data to train AI without explicit safeguards or consent violates this principle.

- 1.2 Avoid harm: Harm includes loss of information, property, or reputation. Using data in ways that risk leaks directly contradicts this.

IEEE Code of Ethics

- I.1 To hold paramount the safety, health, and welfare of the public: Mishandling sensitive data could cause harm to stakeholders, violating this duty.

- I.5 To improve the understanding of technology, its appropriate application, and potential consequences: Professionals must disclose risks of AI models trained on sensitive company data.

- I.7 To seek, accept, and offer honest criticism of technical work: Transparency about how data is used for AI training supports accountability.

1. **Issue:** If the AI's limitations are hidden or its forecasts overstated, users may trust it blindly.
2. **Category:** Honesty and Integrity
3. **Potential Consequences:** Misleading users damages trust, risks lawsuits, and undermines credibility.
4. **Stakeholders Affected:** Clients, regulators, investors.
5. **Impact:** Medium–High risk.
6. **Relevant Professional Codes:**
    - **ACM 1.3:** Be honest and trustworthy.

    - **IEEE I.5:** Clarify appropriate application of technology

1. **Issue:** Poor predictions due to biased, outdated, or incomplete training data could mislead businesses.
2. **Category:** Safety and Health (Financial well-being)
3. **Potential Consequences:** Incorrect forecasts could cause job loss, poor investments, or even business failure.
4. **Stakeholders Affected:** Small business owners, employees, startup founders, investors.
5. **Impact:** High risk — financial stability and livelihoods depend on reliable outputs.
6. **Relevant Professional Codes:**
    a. **ACM 1.2:** Avoid harm.

    b. **IEEE I.5:** Improve understanding of technology's consequences.

Strategies and Justifications

1. **Issue:** The use of your company's data to populate the AI with information to then make predictions for you in the future, but also for others in the future.
2. **Strategy:**

a. Establish strict data governance policies that prohibit company data from being used to train or improve external AI models without explicit contractual safeguards.
b. Require AI vendors to provide opt-out guarantees, ensuring company data is used only for the organization's purposes and not shared with others.
c. Implement data anonymization and minimization before sending information into AI systems, removing identifiers and sensitive business details.
d. Conduct employee training on proper AI tool usage, emphasizing which data can and cannot be shared.

3. **Justification:**

The above proposed strategy is sufficient because and involves proper representation from all angles. Firstly, by getting ahead of any potential issues, by including vendor agreements and ensuring anonymity is upheld, and next, with mitigation, such as the ability to opt out. And least of all, by ensuring that all workers and programmers around the AI have the proper education to ensure company data is always being handled with the utmost care.

1. **Issue:** If the AI's limitations are hidden or its forecasts overstated, users may trust it blindly.
2. **Strategy:**
   a. Provide transparent dashboards that explain how predictions are generated.
   b. Regularly report system error margins and confidence intervals.
   c. Avoid manipulative features designed to steer financial decisions.
3. **Justification:**
   Transparency and honesty build user trust and prevent reliance on misleading forecasts. Clear communication ensures stakeholders make informed decisions.

1. **Issue:** Poor predictions due to biased, outdated, or incomplete training data could mislead businesses.
2. **Strategy:**
   a. Validate data sources regularly and retrain AI models frequently.
   b. Use disclaimers and highlight confidence levels in predictions.
   c. Require human review for high-stakes financial recommendations.
3. **Justification:**
   These steps reduce reliance on flawed data, ensure predictions remain current, and balance automation with human oversight.

Conclusion

Effectiveness of the Strategies:
We will assess the effectiveness of the proposed strategies through continuous monitoring, testing, bias testing and regular reports of how company data is being accessed, shared, and processed by our AI system. We will check that our system is compliant with vendor agreements, free of unauthorized data usage, consistent with the financial data and is successful in security assessments. Our strategies of combining preventative measures and regular checks, we can ensure that the risks are manageable and ethical obligations are met.