Information and Consent to Participate in a Research Study

A. PURPOSE
The purpose of this research is to evaluate the feasibility, perceived benefits, and implementation challenges of draft AI usage policies for software bug fixing from a managerial perspective. By assessing managers' views on enforcing these policies, their concerns, and their preferences across varying organizational policy conditions, this study aims to uncover practical insights for shaping enforceable and effective AI governance in software engineering.

B. PROCEDURES
The study will take approximately 10 minutes to complete. Participants will be asked to fill out an anonymous online survey consisting of multiple-choice and open-ended questions exploring their experiences with proposed AI usage policies for bug fixing, specifically regarding disclosure practices and human oversight. Questions will cover perceptions of feasibility, implementation challenges, and trust in AI under different policy conditions. Participation is voluntary. The survey will be conducted via the SurveyMonkey platform (Here is a link to the privacy policy of the platform.)

C. RISKS
There are no known risks to participation.
D. BENEFITS
You may not personally benefit from participation, but your input will help shape ethical guidelines and frameworks for AI-driven development practices.

E. CONFIDENTIALITY
Your responses will be anonymous, and no personal information (e.g., name or email) will be collected. Any quoted feedback will be anonymized. All data will be securely stored in OneDrive for five years post-publication, after which it will be destroyed.

F. CONDITIONS OF PARTICIPATION
Participation is voluntary, and you may withdraw at any time by closing your browser. Once submitted, responses cannot be withdrawn due to anonymity.

* 1. By choosing "I give my consent" below, you are indicating that you

- Have read and understand the Consent Form provided to you.
- Consent to participate in the research project.
- Understand that a copy of this consent form is available to you for your records.

Do you give your consent?

- ◯ I give my consent
- ◯ I do not give my consent

Demographic Information

In this section, we invite you to share a few details about your background. Your responses will help us better understand the context behind your experience and perspectives on AI usage.

* 2. Please select your age group.

- ◯ Under 18
- ◯ 18 - 24
- ◯ 25 - 34
- ◯ 35 - 44
- ◯ 45 - 54
- ◯ 55 or above

* 3. To which gender identity do you most identify?

- ◯ Woman
- ◯ Man
- ◯ Transgender Woman
- ◯ Transgender Man
- ◯ Gender Variant/Non-Conforming
- ◯ Prefer Not to Answer
- ◯ Prefer to self-describe (Please specify)

* 4. Which country are you currently living in?

* 5. Which of the following best describes your current role or affiliation in the software industry?

- ◯ CEO / Founder / Executive Director
- ◯ CTO / VP of Engineering
- ◯ Engineering Manager / Team Lead
- ◯ Project / Product Manager
- ◯ QA / Test Manager
- ◯ DevOps / Infrastructure Manager
- ◯ Compliance / Risk Manager
- ◯ Other (please specify)

* 6. How many years of expertise do you have in a leadership/managerial role?

- ◯ Less than 1 year
- ◯ 1 - 3 years
- ◯ 4 - 6 years
- ◯ 7 - 10 years
- ◯ More than 10 years

* 7. What is the size of your organization based on the number of employees?

- ◯ 1–10
- ◯ 11–50
- ◯ 51–200
- ◯ 201–500
- ◯ 501–1000
- ◯ 1001+
- ◯ Not applicable / I am not currently working in an organization

* 8. What best describes your role in incorporating policies or rules for technology adoption in your organization?

- ◯ Fully responsible – I directly create and enforce policies.
- ◯ Shared / Advisory role – I contribute to policy design or enforcement but share responsibility with others.
- ◯ Consultative role – I provide input or advice, but final decisions are made by others.
- ◯ Not involved – I do not participate in policy-related decisions.
- ◯ Other (please specify)

[ ]

Policy

The following sections describe high-level summaries of two example policies designed to support responsible and transparent use of AI tools in software bug fixing from a broader perspective. Please read them carefully to have some idea of the content of each policy. You will be asked to reflect on the feasibility, challenges, and your perception of implementing these in a real-world software development environment.

The following definitions are for your understanding to answer the questions in this section.

Disclosure Levels:

- **No Disclosure**: AI usage is never recorded or communicated.
  Example: "I used the LLM to write this patch but didn't mention it in the commit or docs."
- **Partial Disclosure**: Some details about AI usage are shared, but not fully.
  Example: "I noted that I got help from the LLM but didn't explain when or how."
- **Full Disclosure**: All relevant details of AI usage are documented and visible.
  Example: "I documented the prompt, response, and rationale in the code comments and repo log."

Human Oversight Levels:

- **No Human Oversight**: AI fixes are used directly without human review.
  Example: "I copied the LLM output and merged it without checking."
- **Partial Human Oversight**: AI fixes are reviewed or tested, but not fully validated.
  Example: "I checked that it runs, but I didn't have time for code review or security tests."
- **Full Human Oversight**: Fixes go through complete review, testing, and human validation.
  Example: "I reviewed the LLM fix, ran unit tests, and got a teammate to approve it before merging."

* 9. If your organization were to adopt AI tools, what level of *disclosure* would you expect when using an LLM for bug fixing?

	No Disclosure	Partial Disclosure	Full Disclosure
LLM Usage Purpose	○	○	○
LLM Code Contribution	○	○	○
LLM Usage Pattern	○	○	○
LLM Usage Restriction	○	○	○
Disclosure Channel	○	○	○
Disclosure Access Level	○	○	○

* 10. What concerns would you face when mandating full *disclose* of LLM involvement?

- [ ] Increased reporting burden – developers may find disclosure time-consuming or disruptive
- [ ] Reduced productivity – slowing down delivery timelines due to added compliance steps
- [ ] Resistance from developers – pushback or reluctance to follow disclosure rules
- [ ] Difficulty in monitoring compliance – challenges ensuring disclosures are accurate and consistent
- [ ] Risk of superficial disclosures – developers may comply formally without providing meaningful details
- [ ] Impact on trust and autonomy – developers may feel micromanaged or less empowered
- [ ] Confidentiality and legal risks – over-disclosure could reveal sensitive information
- [ ] Other (please specify)

* 11. What trade-offs do you see between being transparent and staying compliant when mandating an *AI usage disclosure policy* in low-risk vs. high-risk domains?

[For example, in high-risk domains, detailed AI disclosure takes more time and slows development, but it improves accountability and trust.
In low-risk domains, full disclosure can feel like extra work, so minimal disclosure saves time but may reduce transparency.]

High-risk Domain (e.g., authentication, encryption, compliance-sensitive areas)

Low-risk Domain (e.g., UI layout, static content, internal documentation, non-critical front-end features)

* 12. What organizational benefits do you associate with following the *AI usage disclosure* policy?

	Strongly Agree	Agree	Disagree	Strongly Disagree
Disclosing AI usage builds accountability and protects the company legally.	○	○	○	○
Disclosure increases transparency and strengthens trust with clients and stakeholders.	○	○	○	○
Following a disclosure policy improves oversight and reduces organizational risk.	○	○	○	○
Clear disclosure ensures higher reliability by enabling better human review of AI outputs.	○	○	○	○

* 13. What would motivate you most to enforce the *AI usage disclosure* policy in your organization?

- [ ] Regulatory compliance
- [ ] Reducing liability risk
- [ ] Improving client trust and reputation
- [ ] Internal accountability and auditing
- [ ] Other (please specify)

* 14. Please select 'Neutral' to confirm you are paying attention.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

* 15. If your organization were to adopt AI tools, what level of *human oversight* would you expect when using an LLM for bug fixing?

	No Human Oversight	Partial Human Oversight	Full Human Oversight
Code Verification	○	○	○
Sensitive Data Protection	○	○	○
Security and Automated Testing	○	○	○
Review Responsibility	○	○	○
Credit and Liability Evaluation	○	○	○
Final Decision Ownership	○	○	○

* 16. What concerns would you face when mandating full *human oversight* of LLM involvement in bug fixes?

- [ ] Full oversight slows down delivery and reduces development speed
- [ ] Constant human review increases workload and resource costs
- [ ] Strict oversight may discourage developers from using AI tools effectively
- [ ] Oversight requirements could lead to superficial or box-ticking compliance
- [ ] Balancing oversight with trust in developers may create friction in teams
- [ ] Enforcing consistent oversight across all projects may be difficult at scale
- [ ] Other (please specify)

* 17. What trade-offs do you see between speed of delivery and assurance of reliability when mandating the *AI usage human oversight* policy in both low and high-risk domains?

[For example, in high-risk domains, strict human oversight slows delivery because every AI-generated fix requires careful review, but it ensures higher reliability and reduces critical errors.
In low-risk domains, lighter oversight speeds up delivery, but the reduced scrutiny can lead to occasional mistakes being overlooked.]

High-risk Domain (e.g., authentication, encryption, compliance-sensitive areas)

Low-risk Domain (e.g., UI layout, static content, internal documentation, non-critical front-end features)

* 18. What organizational benefits do you associate with following the *AI usage human oversight* policy?

	Strongly Agree	Agree	Disagree	Strongly Disagree
Human oversight improves reliability and reduces the risk of faulty AI-generated fixes.	○	○	○	○
A clear oversight process protects the organization from legal and compliance risks.	○	○	○	○
Human involvement ensures that critical decisions remain aligned with organizational standards.	○	○	○	○
Oversight encourages responsible AI use and prevents over-reliance on automation.	○	○	○	○

* 19. What would motivate you most to enforce the *AI usage human oversight* policy in your organization?

- [ ] Ensuring software reliability and security
- [ ] Meeting industry standards or compliance regulations
- [ ] Protecting brand reputation
- [ ] Knowledge sharing and organizational learning
- [ ] Other (please specify)