AI SAFETY GUIDE FOR HR

Security Risks and Action Plan

TABLE OF CONTENTS

HR TRUST IN AI

3%

Have a high level of trust in AI.

43%

Have a moderate level of trust

58%

Data security is a leading barrier to AI adoption.

John, Amy Sarah. “AI Divide in HR: 38% Embrace AI Technology, While non-AI Users Hesitate, Revealing Significant Gap in Adoption and Understanding.” Wire19, 13 June 2024,

Mineral. (2023). (rep.). 2023-state-of-hr-report.

TOP AI CONCERNS

1

Data Privacy

HR departments handle sensitive employee information. There is concern about how AI systems like ChatGPT handle and protect this data.

2

Accuracy and Bias

AI systems can sometimes exhibit biases based on the data they are trained on. HR professionals are wary of any potential bias in AI-driven decisions.

3

Cybersecurity

There is a risk of AI systems being compromised by cyberattacks, potentially exposing sensitive HR data.

4

Compliance

HR departments must adhere to regulations like GDPR or CCPA. Using AI systems introduces complexities around ensuring compliance with these regulations.

5

Employee Trust

Deploying AI in HR functions may affect employee trust. Concerns arise regarding transparency, fairness, and the impact on employee relations.

WHERE IS HR VULNERABLE?

Scams

AI generated optimized resumes and cover letters are flooding the market with unqualified applicants making talent harder to reach.

Data Compliance

Your industry may have strict data restrictions like HIPAA, CCPA, GDPR that **third party tools** deploying AI don't have.

Sourcing

ChatGPT pulls it's information from **prior to 2021** which means, the information could be largely out of date.

Credibility

Open AI software like ChatGPT do not provide **citations** for the data it's sourcing from.

Data Cleanliness

To use third party applications to deploy functions provided by AI, your data must be **clean**.

Not Regulated, yet.

Once legislation catches up, you will need to **pivot** depending on how much AI integration you've done and what the regulation is.

Sommer, Brian President TechVentive, Inc.
The Dark Side of HR, 17 July. 2024. Webinar.

5 ETHICAL AND PRIVACY CONSIDERATIONS

1. What's your company's **ethical boundaries**?
2. Do employees know what data is being **collected**?
3. How is employee's information being **used**?
4. How will **privacy** will be safeguarded?
5. When is AI **making-decisions**?

HOW TO NAVIGATE SAFELY

Don't Over Rely on AI

AI needs human guidance for **decision-making** and to check the data/process. Always add in human checks and balances.

Start Small

Start with **non-confidential** or non-prioprietary information like summarizing job interviews or taking meeting notes.

Integrate Slowly

As we wait for regulation, it's better to implement **slowly** on less critical parts of the business to avoid friction for your workforce.

Create a Strategy

Lay out a plan of research, integration, and define **goals**. It will help you to have an understanding about how you're progressing.

Be Transparent

Maintaining trust is critical. Stay **transparent** about your use of AI in your company.

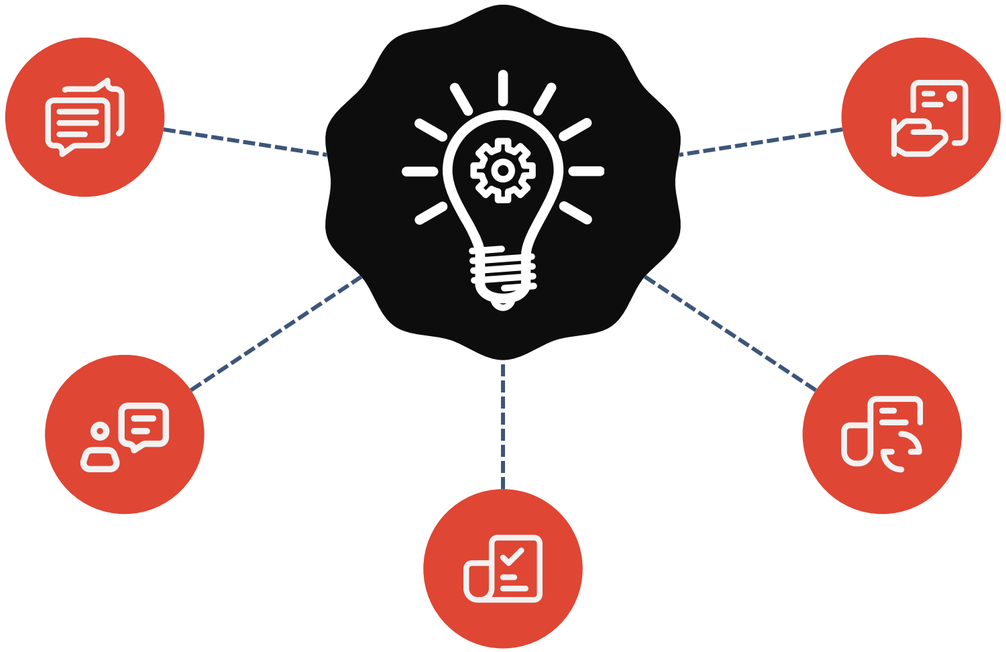
Investigate Vendors

Can your vendor talk about how they use their data, how they **train their model**, and how they validate that it doesn't have an adverse impact? Know how the tool you're using works.

WHAT'S YOUR STRATEGY?

Outline your use policy for AI: When and where you will use AI (even if this process will happen in stages).

Identify processes that don't include confidential information that you can play with.



Build a plan around the risks and provide room to fluctuate based on unknown legislation.

Stay aware of the risks and threats to consider based on your specific use with AI.

Discover where can you expand your knowledge and try out a new tool.
List of the best AI for HR.

ASSESS YOUR RISKS

LITIGATION

It is difficult to defend a new piece of software, and you might need to be ready to prove your safeguards and due diligence to protect employee data.

TO DO:

1. Perform a SWOT (strengths, weaknesses, opportunities, and threats) analysis
2. Consider adding an AI security role to your IT team.
3. Review your disclaimers, privacy policy, and terms of use for AI integration.
4. Ensure your AI tool is compatible with GDPR and/or CCPA and any additional state and industry standards.
5. Anticipate when and where legal advice is needed.

TAKE ACTION

What are your next steps and AI goals?

Step 1 →	Step 2 →	Step 3 →	Step 4 →
LEARN THE THREATS	DEFINE YOUR STRATEGY	ASSESS YOUR RISKS	TAKE ACTION