AI Application Vetting Checklist

This checklist is designed to help organizations assess third-party and internally developed AI applications for compliance, fairness, security, and performance prior to deployment in the workplace.

# 1. Data Integrity and Sourcing

* ☐ Is the training data source lawful, verifiable, and appropriate for the intended use?
* ☐ Has the data been reviewed for bias or representational gaps?
* ☐ Is personal or sensitive data anonymized or protected by privacy safeguards?

# 2. Algorithmic Transparency

* ☐ Can the AI system’s logic and outputs be explained to end-users?
* ☐ Does the vendor provide sufficient technical documentation or a model card?
* ☐ Are there human-readable summaries of decision-making criteria?

# 3. Bias and Fairness Testing

* ☐ Has the AI system been tested for disparate impact across protected classes (race, gender, disability, etc.)?
* ☐ Are bias test results and mitigation strategies documented and available for review?

# 4. Privacy and Security

* ☐ Does the system comply with applicable data privacy laws (e.g., GDPR, CCPA)?
* ☐ Is data encrypted at rest and in transit?
* ☐ Is access to AI-generated data controlled and auditable?

# 5. Performance and Accuracy

* ☐ Has the tool been validated for accuracy, precision, recall, or other relevant metrics?
* ☐ Are error rates monitored and documented?
* ☐ Is the system regularly updated with new data or model improvements?

# 6. Accessibility and Inclusion

* ☐ Is the AI tool compliant with WCAG or ADA standards for accessibility?
* ☐ Is the interface user-friendly for non-technical users or individuals with disabilities?

# 7. Legal and Ethical Compliance

* ☐ Does the tool comply with local, state, and federal employment laws?
* ☐ Is there a process for affected individuals to appeal or request a human review?
* ☐ Are appropriate disclaimers or notices presented to users/applicants?

# 8. Vendor Due Diligence

* ☐ Is the vendor reputable and experienced in the domain of AI application?
* ☐ Does the vendor agree to indemnify the organization against algorithmic harm or legal liability?
* ☐ Are terms related to IP, data ownership, and confidentiality clearly defined in the contract?