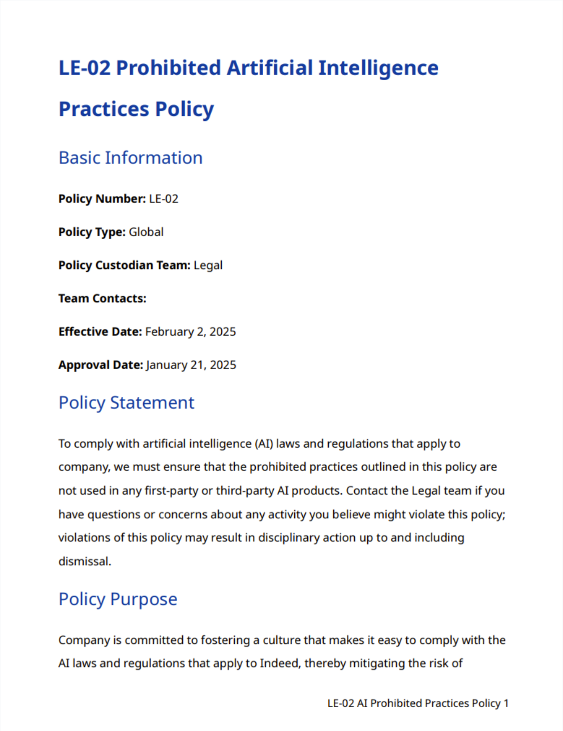
AI Policy & Control Mapping

Enterprise Policy, Control Alignment, and MITRE AI Risk Integration

Enterprise AI Policy Framework

- Formal AI governance policy aligned to EO 14110 and OMB M-24-10
- Risk-tiered model categorization and prohibited use definitions
- Board-level oversight and accountability structure
- Enterprise enforcement standards and monitoring controls



LE-02 Prohibited Artificial Intelligence Practices Policy

Basic Information

Policy Number: LE-02

Policy Type: Global

Policy Custodian Team: Legal

Team Contacts:

Effective Date: February 2, 2025

Approval Date: January 21, 2025

Policy Statement

To comply with artificial intelligence (AI) laws and regulations that apply to company, we must ensure that the prohibited practices outlined in this policy are not used in any first-party or third-party AI products. Contact the Legal team if you have questions or concerns about any activity you believe might violate this policy; violations of this policy may result in disciplinary action up to and including dismissal.

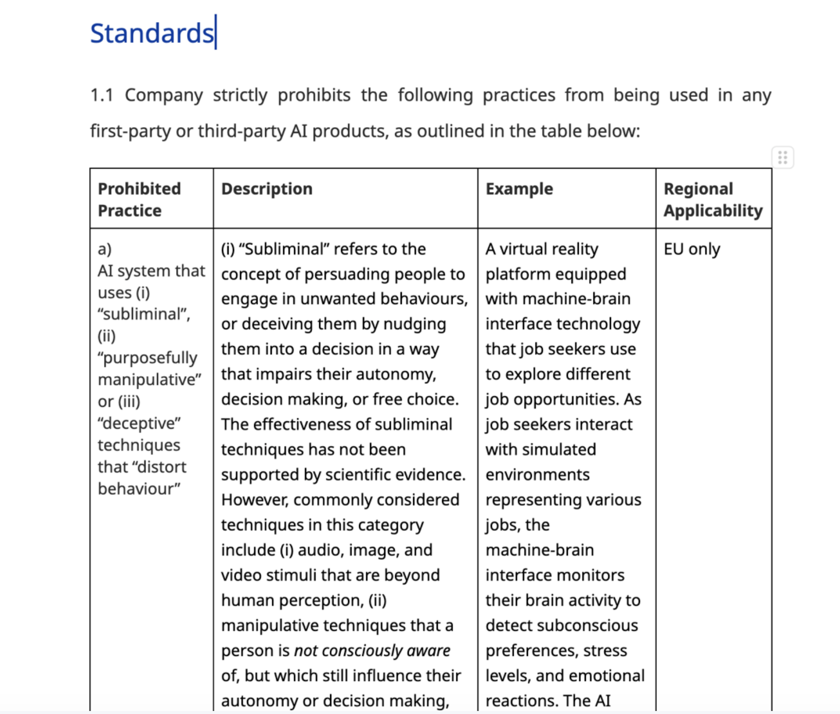
Policy Purpose

Company is committed to fostering a culture that makes it easy to comply with the AI laws and regulations that apply to Indeed, thereby mitigating the risk of

LE-02 AI Prohibited Practices Policy 1

Internal AI Use Policy & Workforce Controls

- Defined acceptable and prohibited AI usage standards
- Data handling, input/output restrictions, and monitoring rules
- Employee attestation and mandatory training integration
- Embedded compliance language for contractors and vendors



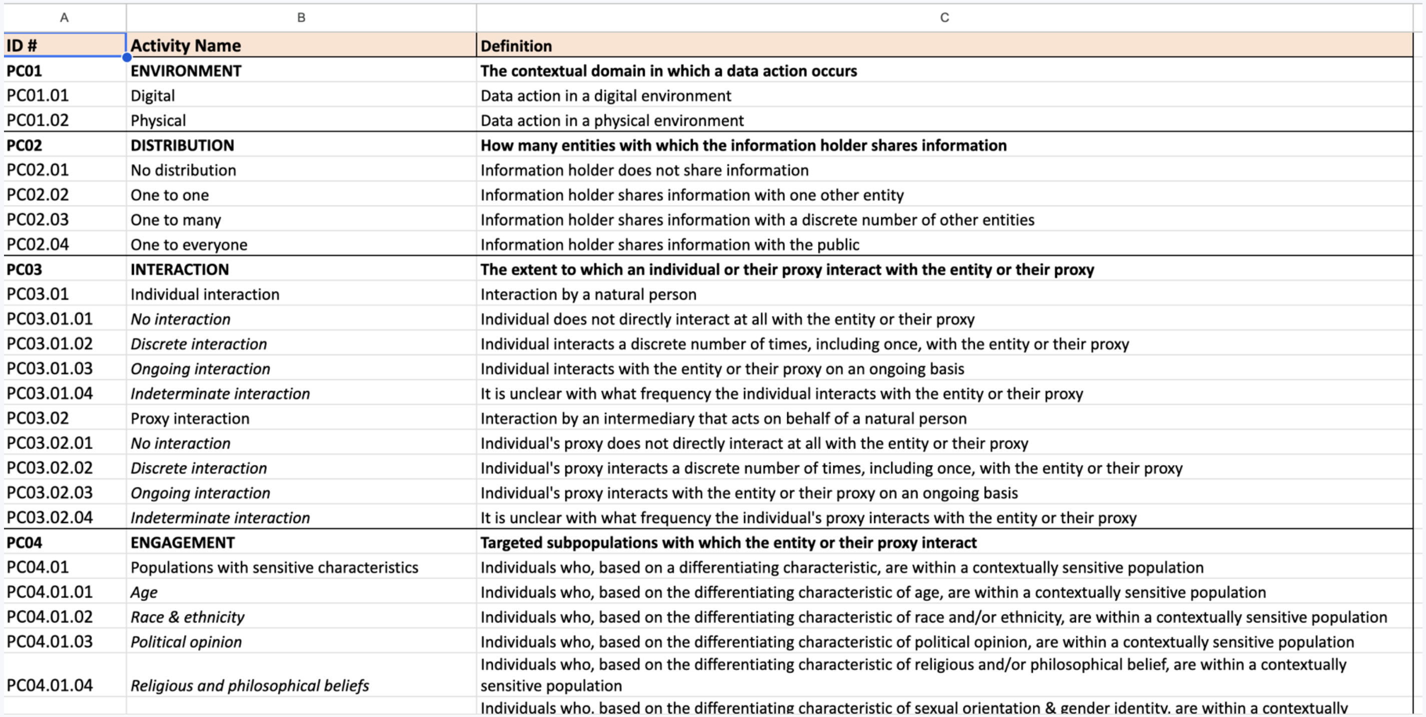
Standards

1.1 Company strictly prohibits the following practices from being used in any first-party or third-party AI products, as outlined in the table below:

Prohibited Practice	Description	Example	Regional Applicability
a) AI system that uses (i) “subliminal”, (ii) “purposefully manipulative” or (iii) “deceptive” techniques that “distort behaviour”	(i) “Subliminal” refers to the concept of persuading people to engage in unwanted behaviours, or deceiving them by nudging them into a decision in a way that impairs their autonomy, decision making, or free choice. The effectiveness of subliminal techniques has not been supported by scientific evidence. However, commonly considered techniques in this category include (i) audio, image, and video stimuli that are beyond human perception, (ii) manipulative techniques that a person is *not consciously aware* of, but which still influence their autonomy or decision making,	A virtual reality platform equipped with machine-brain interface technology that job seekers use to explore different job opportunities. As job seekers interact with simulated environments representing various jobs, the machine-brain interface monitors their brain activity to detect subconscious preferences, stress levels, and emotional reactions. The AI	EU only

AI Control Mapping & Compliance Crosswalk

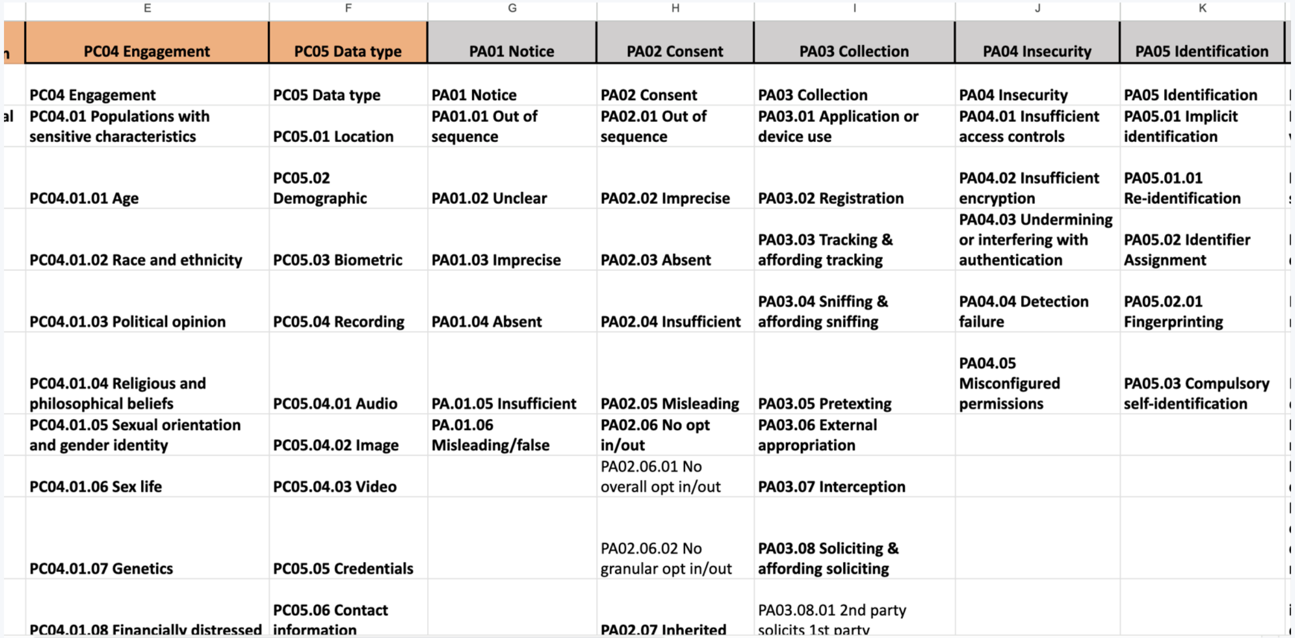
- NIST AI RMF control mapping
- MITRE ATLAS / Panoptic taxonomy alignment
- OMB M-24-10 reporting readiness
- Documented risk classification artifacts



A	B	C
ID #	**Activity Name**	**Definition**
PC01	**ENVIRONMENT**	**The contextual domain in which a data action occurs**
PC01.01	Digital	Data action in a digital environment
PC01.02	Physical	Data action in a physical environment
PC02	**DISTRIBUTION**	**How many entities with which the information holder shares information**
PC02.01	No distribution	Information holder does not share information
PC02.02	One to one	Information holder shares information with one other entity
PC02.03	One to many	Information holder shares information with a discrete number of other entities
PC02.04	One to everyone	Information holder shares information with the public
PC03	**INTERACTION**	**The extent to which an individual or their proxy interact with the entity or their proxy**
PC03.01	Individual interaction	Interaction by a natural person
PC03.01.01	*No interaction*	Individual does not directly interact at all with the entity or their proxy
PC03.01.02	*Discrete interaction*	Individual interacts a discrete number of times, including once, with the entity or their proxy
PC03.01.03	*Ongoing interaction*	Individual interacts with the entity or their proxy on an ongoing basis
PC03.01.04	*Indeterminate interaction*	It is unclear with what frequency the individual interacts with the entity or their proxy
PC03.02	Proxy interaction	Interaction by an intermediary that acts on behalf of a natural person
PC03.02.01	*No interaction*	Individual's proxy does not directly interact at all with the entity or their proxy
PC03.02.02	*Discrete interaction*	Individual's proxy interacts a discrete number of times, including once, with the entity or their proxy
PC03.02.03	*Ongoing interaction*	Individual's proxy interacts with the entity or their proxy on an ongoing basis
PC03.02.04	*Indeterminate interaction*	It is unclear with what frequency the individual's proxy interacts with the entity or their proxy
PC04	**ENGAGEMENT**	**Targeted subpopulations with which the entity or their proxy interact**
PC04.01	Populations with sensitive characteristics	Individuals who, based on a differentiating characteristic, are within a contextually sensitive population
PC04.01.01	*Age*	Individuals who, based on the differentiating characteristic of age, are within a contextually sensitive population
PC04.01.02	*Race & ethnicity*	Individuals who, based on the differentiating characteristic of race and/or ethnicity, are within a contextually sensitive population
PC04.01.03	*Political opinion*	Individuals who, based on the differentiating characteristic of political opinion, are within a contextually sensitive population
PC04.01.04	*Religious and philosophical beliefs*	Individuals who, based on the differentiating characteristic of religious and/or philosophical belief, are within a contextually sensitive population
		Individuals who, based on the differentiating characteristic of sexual orientation & gender identity, are within a contextually

MITRE AI Risk Taxonomy Deliverable

- Full enterprise AI risk taxonomy mapping
- Classification of interaction, data, and insecurity domains
- Embedded audit-ready artifact for federal review
- Control traceability from risk to mitigation



E	F	G	H	I	J	K
PC04 Engagement	**PC05 Data type**	**PA01 Notice**	**PA02 Consent**	**PA03 Collection**	**PA04 Insecurity**	**PA05 Identification**
PC04 Engagement	**PC05 Data type**	**PA01 Notice**	**PA02 Consent**	**PA03 Collection**	**PA04 Insecurity**	**PA05 Identification**
PC04.01 Populations with sensitive characteristics	**PC05.01 Location**	**PA01.01 Out of sequence**	**PA02.01 Out of sequence**	**PA03.01 Application or device use**	**PA04.01 Insufficient access controls**	**PA05.01 Implicit identification**
PC04.01.01 Age	**PC05.02 Demographic**	**PA01.02 Unclear**	**PA02.02 Imprecise**	**PA03.02 Registration**	**PA04.02 Insufficient encryption**	**PA05.01.01 Re-identification**
PC04.01.02 Race and ethnicity	**PC05.03 Biometric**	**PA01.03 Imprecise**	**PA02.03 Absent**	**PA03.03 Tracking & affording tracking**	**PA04.03 Undermining or interfering with authentication**	**PA05.02 Identifier Assignment**
PC04.01.03 Political opinion	**PC05.04 Recording**	**PA01.04 Absent**	**PA02.04 Insufficient**	**PA03.04 Sniffing & affording sniffing**	**PA04.04 Detection failure**	**PA05.02.01 Fingerprinting**
PC04.01.04 Religious and philosophical beliefs	**PC05.04.01 Audio**	**PA.01.05 Insufficient**	**PA02.05 Misleading**	**PA03.05 Pretexting**	**PA04.05 Misconfigured permissions**	**PA05.03 Compulsory self-identification**
PC04.01.05 Sexual orientation and gender identity	**PC05.04.02 Image**	**PA.01.06 Misleading/false**	**PA02.06 No opt in/out**	**PA03.06 External appropriation**		
PC04.01.06 Sex life	**PC05.04.03 Video**		PA02.06.01 No overall opt in/out	**PA03.07 Interception**		
PC04.01.07 Genetics	**PC05.05 Credentials**		PA02.06.02 No granular opt in/out	**PA03.08 Soliciting & affording soliciting**		
PC04.01.08 Financially distressed	**PC05.06 Contact information**		**PA02.07 Inherited**	PA03.08.01 2nd party solicits 1st party		

Board-Ready AI Governance Infrastructure

Policy | Controls | Risk Mapping | Federal Alignment