

GENERATIVE ARTIFICIAL INTELLIGENCE RISK ASSESSMENT
HBEX 707 (04/25)

GENERATIVE ARTIFICIAL INTELLIGENCE RISK ASSESSMENT

The Generative Artificial Intelligence (GenAI) Risk Assessment form is used by Covered California to evaluate and mitigate potential risks associated with the use and if applicable, procurement of GenAI technologies. This form helps ensure that any new GenAI tool or software aligns with our data privacy, security, and ethical standards. By completing this form, requestors and vendors provide essential information regarding their GenAI solutions' capabilities, data handling practices, and safeguards. The objective is to proactively identify and address any privacy concerns, security vulnerabilities, or ethical dilemmas associated with integrating or utilizing GenAI within Covered California.

Section 1: Vendor/Software/Use Case(s) to be completed by the Covered California Requestor

Requester Name: _____

Date Submitted: _____

This form is to be completed when evaluating or procuring software. If this request doesn't include software, please mark the box below and return it to the requestor.

This request does not include software

Vendor Information

Vendor Name:

Software Name:

Type of Request: *Is it an add-on capability to an already approved tool/software at Covered California? If yes, specify what is being added.*

Business Problem for the Requested Tool/Software: *What is the use case(s) for the requested tool/software? For each business problem, specify which division/function(s) it enables.*

Data Privacy Considerations

Will Personal Identifiable Information be accessible to the GenAI tool? If yes, describe the type of data.

Section 2: GenAI Risk Assessment to be Completed by Vendor

Contact Name: _____

Contact Phone: _____

Contact Email: _____

Will you and/or your subcontractor(s) use or offer GenAI technology, model, service, or system?

☐ Yes ☐ No (If no, skip to the Signature section of this form)

Tool/Software Description

Description of tool/software, including product description. *Provide a general description of the tool/software, including its primary functions and intended use cases.*

LLM Models and Entity Affiliations. *List all GenAI models (incl. model name, model version, and number of parameters), as well as owners and entities associated with this solution.*

- LLM Model Name(s): _____
- LLM Model Version Number(s): _____
- LLM Model Parameters: _____
- LLM Entity Owner: _____

Hosting, Data Storage, and Security

Question	Instructions	To be completed by vendor
Where is the software hosted?	<i>Specify the hosting environment for the software (e.g., on-premises, private cloud, public cloud, or other). If cloud-hosted, provide the name of the service provider (e.g., AWS, Azure, GCP) and the geographic location of the data centers / environments used.</i>	Hosting Environment If other, please specify: Provider Name:
Where is the foundational model (e.g., LLM) hosted?	<i>Indicate where the foundational model (e.g., Large Language Model (LLM)) is hosted. If cloud-based, specify whether it operates in a multi-tenant or single-tenant environment. If on-premises, describe the security controls in place.</i>	
Is customer data stored in a private or shared instance? If private, is the data sent outside of those boundaries?	<i>Specify whether customer data is stored in a private or shared instance. If private, clarify whether data processing occurs solely within that instance or if data is transmitted to external environments for processing, analysis, or model refinement.</i>	
Where will the data sources come from and what is the retention policy for customer data?	<i>Identify all data sources feeding into the GenAI system, including structured and unstructured data. Specify data retention policies, including duration, storage locations, compliance with regulatory standards (e.g., GDPR, CCPA), and data deletion procedures.</i>	

Data Usage, Privacy, and Security

Question	Instructions	To be completed by vendor
Is customer data used to train or refine the foundational model or application? If yes, describe how this data is anonymized.	<i>Does the system use customer data for model training, fine-tuning, or continuous learning? If so, detail data anonymization and differential privacy techniques applied, including whether data is stored in a federated learning framework or used for direct model updates.</i>	

What security policies / mechanisms does your solution have in place to prevent unauthorized access to customer data?	<i>Specify all security policies and mechanisms/tools in place to prevent unauthorized access to customer data (e.g., RBAC), both within organization and by end-users of the software/tool.</i>	
What is the risk of customer data being leaked to the public or unauthorized individuals?	<i>Assess the risk level of customer data exposure due to security vulnerabilities, model inversion attacks, or data extraction techniques. List existing mitigation measures, including encryption, access controls, and monitoring tools.</i>	
When is the last time you had a security assessment and penetration testing? What was the outcome from the assessment and test?	<i>Provide the date of the most recent security audit and penetration testing. Include details on the scope of testing (e.g., adversarial AI testing, red teaming) and any high-severity vulnerabilities identified.</i>	
Can users opt out of data collection, processing or inference by the foundational model?	<i>Describe mechanisms/ information available to inform users of data usage.</i> <i>Describe any opt-out mechanism in place, including whether these applies globally or per-use session.</i>	
What is your general privacy policy?	<i>Provide a link to your company's privacy policy.</i>	
What is your GenAI privacy policy?	<i>Provide a link to your company's GenAI privacy policy,</i>	

Ethical AI/Bias Prevention Guardrails
--

Question	Instructions	To be completed by vendor
Explain how the system prevents bias and remains ethical.	<i>Explain how the system prevents bias and ensures ethical decision-making, considering the following factors:</i> <i>Data sourcing and diversity: Describe measures to ensure training data represents diverse demographics and avoids systemic biases.</i> <i>Model fairness techniques: Explain bias mitigation strategies such as adversarial debiasing, reweighting, or fairness-aware loss functions.</i> <i>Human oversight: Detail how human-in-the-loop (HITL) methods are applied to validate AI decisions and detect potential ethical risks.</i> <i>Compliance and governance: Outline how the system adheres to ethical AI frameworks, such as NIST AI Risk Management, OECD AI Principles, or the EU AI Act.</i>	
Explain how the system ensures outputs are explainable.	<i>Describe what measures are in place to ensure outputs are explainable (e.g., citations / ability to trace reference sources).</i>	
Explain how the system prevents inaccurate outputs.	<i>Explain how the system prevents false or misleading outputs (i.e., hallucinations) which may undermine decision-making.</i>	
Explain how the system prevents incorrect/ malicious use.	<i>Is there a risk that the application or foundational model could generate harmful, misleading, or non-compliant outputs? If so, describe safeguards such as adversarial robustness testing, response filtering, and reinforcement learning from human feedback (RLHF).</i>	

By signing this document, I have identified and reported where Covered California may use GenAI regarding the above-mentioned tools/software. If any new or previously unreported GenAI use is identified in the future, we will notify the Covered California contract manager and initiate a new GenAI risk assessment.

Full Printed Name:**Title:**

--	--

Signature:**Date:**

--	--