Acceptable Use Policy for AI Tools

Purpose

Artificial Intelligence ("AI") tools like generative AI (e.g., ChatGPT) and large language models (e.g. Meta Llama) or (collectively, "AI Tools") have numerous applications that can assist in data management, writing or modifying software code, and generally improving workplace efficiency. However, AI Tools come with cybersecurity, privacy and data risks, and the improper use of these tools can expose Tesla's proprietary information, reveal personal data, violate local laws, and/or break third party confidentiality commitments.

Scope

This Policy applies to all Tesla Workers who have access to Tesla's data, systems or network. AI Tools used by Workers for executing job responsibilities are within the scope of this Policy. AI Tools built by Tesla (referred to as the 'Company' henceforth) for commercial use on Tesla products (e.g., Optimus, Autopilot) are not in scope of this Policy.

Responsibility

The ownership of this Policy along with its corresponding security requirements is the responsibility of Information Security under the Leader of Information Security. This Policy shall be reviewed periodically and formally approved by the Leader of Information Security, with the assistance of the Governance Risk Compliance function and the Data Privacy function of Tesla. Additionally, it is the responsibility of all Workers to adhere to this Policy.

Policy

This Policy places limitations on the data provided to AI Tools as well as how their output is handled.

It is acceptable to use Approved AI Tools to improve productivity, as long as Tesla Data is strictly limited to use within the tools mentioned in **Table 1** below. Any usage of such data must be in full compliance with local laws, information security, privacy and all Tesla policies. Workers must be transparent about the use of AI Tools in their work, by clearly attributing AI use notice. For any questions on the use of AI Tools in compliance with local laws, please contact your local legal counsel, privacy@tesla.com or infosec@tesla.com.

The following sections provide additional details of this Policy via specific scenarios and use cases to help better understand the limitations.

1. Approved AI Tools
While it is impractical to list every approved tool, key tools will be highlighted to illustrate the classes of tools and options.

Table 1: Approved AI Tool Type and respective Tesla Data Usage Permissions

Tool Type	Tesla Data usage allowed in prompts?
Tesla Approved Tools	**Yes** Refer to "Approved Software – AI Tools"
Conditionally Approved Tools	**No*** Refer to "Approved Software – AI Tools"

* Additional restrictions apply to Conditionally Approved Tools when working with Tesla Code. See "Prohibited Uses of AI Tools" section.

A list of Approved Tools can be found at Confluence "Approved Software - AI Tools" (Link: https://go.tesla.com/aitools).

Note: If the AI Tool is not featured on above link or is not explicitly approved, its usage is prohibited.

Below are examples of **Tesla Approved Tools**:

a. The general-purpose AI chatbot is https://go.tesla.com/chat
b. Some departments have implemented their own approved AI chat bots such as
    - IT Assist https://it.bottlerocket.tesla.com
    - Employee Assist https://hr.bottlerocket.tesla.com
c. Inferencing as a service is available to teams that want to control their entire implementation stack end to end. Please refer to https://go.tesla.com/inference for more details.

2. Unapproved AI Tools
Self-hosted models on-premises are not approved without ARB and cost justification. This includes self-hosted models such as Llama, DeepSeek, OJan/Msty. Self-hosted and do it yourself solutions are generally not cost effective, overlap with other solutions and often lack standard controls, logging, reliability support, and privacy capabilities. There are several optimized, supported, approved methods available. Special use cases can be evaluated via ARB process. Please see: https://go.tesla.com/ARB.

Prohibited Use of AI Tools

Sharing or uploading any Tesla Data (including Personal Data of Tesla employees, customers, or vendors), or Data classified as Sensitive or Confidential Business Data per Data Classification and Management Policy, to Unapproved or Conditionally Approved Tools is prohibited.

Additional prohibited uses include:

1. Providing any Tesla Code as input to Unapproved or Conditionally Approved AI Tools for purposes such as
    a. Running tests on Tesla Code
    b. Debugging Tesla Code

    c. Optimizing Tesla Code
    d. To sort through Tesla databases or ERP systems
    e. Any other use case where Tesla Code is provided as input
2. Creating outputs (e.g., presentations, training material, service documents) with unapproved or third-party AI Tools if the input materials contain Tesla Data or other non-public information.
3. Use of unapproved mobile phone-based Intelligence tools, including Apple Intelligence, on Tesla-issued (corporate) devices.
4. Use of AI Tools to record or transcribe meetings as part of conducting Tesla business is prohibited. The restriction applies to all parties involved in the meetings (including third-party suppliers and Tesla internal). Please see the Global Meeting Recording Policy.
5. Use of AI aids such as notetaking/transcribing from either party during interviews. Candidates applying for a position at Tesla are required to clear all interview rounds without the use of AI Tools. Hiring managers are encouraged to be wary of such malpractices and employ steps/controls to deter the same.
6. **Video, Photography, Audio:** As per your signed Code of Business Ethics and employee NDA, taking photos or recording images inside Tesla facilities that could publicly expose Tesla Business Information is prohibited. Devices that fall under this restriction include but are not limited to: Ray-Ban Meta Glasses, AI-powered standalone recording / transcription devices, etc. For additional details, refer to Code of Business Ethics - **"Protect Information and Assets" section**.

Acceptable Uses of AI Tools

Listed below are examples of acceptable use cases, to serve as a guideline. Employees may use Approved AI Tools as long as the requirements in this Policy are met:

1. As an internet search engine
2. To summarize complex, publicly available information
3. To assist in writing text
4. To assist with mathematical calculations
5. To assist in writing code (e.g., write a program to find max value in Python)

Note: Tesla Data is only permitted for use in Tesla Approved Tools. The use of Tesla Data, including information covered by NDA or unreleased data, is prohibited with Tools in the "Conditionally Approved" type. For more details, please refer to **Table 1** above which outlines the Approved Tools Type and their respective Tesla Data Usage Permissions. Please see "Approved Software – AI Tools" for the comprehensive list of AI Tools.
For any questions on the use of AI Tools, please contact infosec@tesla.com.

Responsible Use of AI-Generated Data

AI models may produce inaccurate or unfounded information due to biased or incomplete training data. Workers are responsible for understanding the limitations of AI-based Tools, reviewing/validating the output, and exercising due diligence before using any output generated from internal and approved third party AI Tools.
Workers must be transparent about the use of AI Tools in their work, by clearly attributing AI use notice.

All code, including AI assisted or generated must adhere to Tesla's secure coding best practices:

a. AI-generated code must be reviewed by the user and peer reviewed
b. AI-generated code must not contain potentially dangerous content
c. AI-generated code must not violate copyright/license terms
d. AI-generated code should go through:
    - Application security scans
    - Testing
    - Peer review

For information refer to Tesla Baseline Internal-Apps Security Requirements Policy and Security Guidelines.

Exception

For requesting exceptions to this Policy reach out to infosec@tesla.com and visit https://go.tesla.com/ARB.

Non-Compliance

Tesla reserves the right to take legal action or press charges against users whose use of AI Tools is violating local, state or federal laws. Workers who violate this Policy may be subject to disciplinary action, up to and including termination. Questions regarding this Policy should be directed to infosec@tesla.com.

Definitions

Tesla Data – Any and all information, data (including Personal Data), materials, works or content regarding Tesla, Tesla customers, Tesla affiliates, Tesla employees or its users.

Tesla Code – Any piece of code that is merged into Tesla code repositories, i.e, code of internal/external applications, services, microservices, portals, API, etc.

Personal Data – Any information that relates to an identifiable or identified individual (e.g., customer, employee, vendor point of contact).

Tesla Workers – All Tesla employees and workers, including interns, contingent workers, contractors, part time and full-time employees.

Revision History

Date	Author	Action Taken	Version
07/05/2023	Manager, IT Security & Compliance	Document Creation	1.0
07/18/2023	Director, Product Security Engineering	Approval	1.0
07/27/2023	Director, Security Intelligence	Approval	1.0
07/31/2023	Deputy General Counsel (Legal)	Approval	1.0
07/31/2023	Privacy Legal (DPO)	Approval	1.0
08/02/2023	Head of IT Security	Approval	1.0
07/05/2024	Manager, IT Security & Compliance	Document Creation	1.1
06/19/2024	Director, Product Security Engineering	Approval	1.1
06/19/2024	Director, Security Intelligence	Approval	1.1
07/29/2024	Deputy General Counsel (Legal)	Approval	1.1
08/06/2024	Privacy Legal (DPO)	Approval	1.1
02/12/2025	1. GRC InfoSec Compliance Lead 2. Manager, SME, Information Security	Revision	2.0
03/27/2025	Privacy Legal (DPO)	Approval	2.0
04/29/2025	Leader of Information Security	Approval	2.0