TRINITY INDUSTRIES	Document	IRM-070-POL-EN
	Version	1.0.1
	Published Date	2025-03-03
	Effective Date	2025-03-03
	Document Owner	Chief Information Security Officer / B. Mork

Responsible Use of Artificial Intelligence Policy

1. PURPOSE

The purpose of this document is to establish boundaries for the responsible use of Artificial Intelligence (AI) technologies by Trinity. It aims to ensure that AI is utilized in a manner that upholds legal and ethical standards, respects intellectual property rights, and promotes accountability. This document will be updated in accordance with the **Enterprise Document Management Policy (DMS-001-POL-EN)**.

2. SCOPE

This policy is in full force and effect throughout all business operations of Trinity Industries, Inc., its subsidiaries, and affiliates (collectively “Trinity”).

3. DEFINITIONS

General Information Security terms are defined in **Information Risk Management Definitions Standard (IRM-016-STD-EN)**. The following terms have unique definitions applicable solely within this document and to this policy.

- **Artificial Intelligence** is used in this document to mean any technical implementation that performs tasks or analysis with a degree of complexity that traditionally required a human intellect.
- **Authorized User** is used in this document to mean any individual (inclusive of employees, contractors, partners, customers, and Third Parties) who has been appropriately authorized to access Trinity Data.
- **Business Process Owner** (BPO) is used in this document to mean the functional owner that is responsible for directing a process area to meet regulatory and business requirements.
- **Computing Asset** is used in this document to mean any physical or virtual system or service –inclusive of but not exclusive to laptops, desktops, servers, networking devices, mobile devices, storage devices, embedded solutions, and containers – that stores, accesses, processes, or transmits Trinity Data in an unencrypted format.
- **Data Owner** is used in this document to mean an officer of Trinity or an individual delegated by an officer of Trinity to identify one or more types of Trinity Data, as well as the controls and processes necessary to protect such data.
- **IT Services** is used in this document to mean any software, firmware, service, networking technology, Computing Asset, or solution which processes, stores, or transmits Trinity Data. IT Services explicitly includes all Computing Assets, Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and any software, executable code, or firmware installed on Trinity Computing Assets regardless of whether owned or operated by or on behalf of Trinity.
- **Personally Identifiable Information** (PII) is used in this document to mean any information that can be used to clearly identify a particular individual or household. PII is inclusive of (A) “personal information” as defined under the California Consumer Privacy Act (CCPA) of 2018, including, but not limited to unique personal identifiers such as email addresses, telephone numbers, browsing history, education information, employment history, and financial information and (B) “sensitive personal information” as defined under the California Privacy Rights Act (CPRA) of 2020, including, but not limited to social security numbers, precise geolocation, credit or debit card information, race or ethnic origin, health and genetic data, and email/message contents. Additional privacy laws and definitions may also apply based on upon region or country, including, but not limited to, Mexico’s Federal Law on the Protection of Personal Data Held by Private Parties. Please consult the Legal Department for questions regarding international privacy laws.
- **Third Party** is used in this document to mean any entity or individual not directly owned, operated, or employed by Trinity. Contingent labor personnel are not considered to be Third Parties within this document.

- **Trinity Data** is used in this document to mean any non-public data or information owned, held, or controlled by Trinity, inclusive of PII and information or data from Third Parties.

4. STATEMENT OF POLICY

The use of Artificial Intelligence (AI) must minimally conform to the same standards of acceptability that apply to traditional use of IT Services, as established in the **Information Security Policy (IRM-003-POL-EN)**, the **Vulnerability Management Policy (IRM-006-POL-EN)**, the **Global Logging Policy (IRM-010-POL-EN)**, the **Data Classification Policy (IRM-012-POL-EN)**, and the **Acceptable Use Policy (IRM-002-POL-EN)**.

4.1. USE OF AI

Any use of Trinity Data by an AI that is not fully contained within Trinity IT Services or within environments operated exclusively by a contracted Third Party on behalf of Trinity is explicitly prohibited. The use of an AI for general queries that do not involve the submission or processing of Trinity Data is generally permissible. Any use of AI that will involve Trinity Data must take place only once the following conditions have been met:

1. A contract is in place between the provider of the AI and Trinity that has been reviewed and approved by the Legal, Ethics and Compliance (E&C), Information Risk Management (IRM), and IT organizations.
2. A Business Process Owner (BPO) has been identified and documented within Trinity who will be responsible for the ongoing review and compliance of the AI implementation.
3. The AI has been approved following an AI Technology Review. (Section 4.4)
4. The AI has been approved following an AI Ethical Assessment. (Section 4.5)

The use of AI does not remove the responsibility of employees, contractors, consultants, and similar labor providers relating to quality or accuracy of work. All personnel are responsible for ensuring that outputs from an AI are fact checked, appropriate, and applicable prior to making any business decisions.

4.2. INTELLECTUAL PROPERTY PROTECTION

Trinity recognizes the significance of intellectual property (IP) protection in the field of AI. All AI technologies, algorithms, models, codebases, files, and related documentation created, developed, or acquired by Trinity are considered proprietary assets. All Trinity employees and stakeholders are required to respect and uphold Trinity's IP rights (including local and international regulations) and take necessary steps to safeguard these proprietary assets including IP arising from the development or use of AI as well as from the use of other IP with AIs or AI-enabled technologies/solutions.

Collaboration with external experts, research institutions, educational institutions, and regulatory bodies on AI is only permitted with the explicit agreement of the Chief Legal Officer (CLO) and after executing appropriate business or service agreements and non-disclosure agreements to protect the IP rights and interests of Trinity. The CLO shall be the sole authority in determining what constitutes an appropriate agreement with regard to IP rights and interests.

4.3. INTERNAL AI USE

Customizable AI technologies developed or utilized by Trinity shall not be installed or instantiated on systems that are not fully controlled by Trinity. This includes installation or instantiation to third-party platforms, open-source projects, and external environments where Trinity lacks sufficient oversight. This restriction is imposed to safeguard against potential misuse, data breaches, and unanticipated consequences arising from AI use in uncontrolled settings.

4.4. AI TECHNOLOGY REVIEWS

AI Technology Reviews must include reviews by the IRM organization, E&C department, and the broader Legal department prior to any use. IRM, E&C, and Legal approvals must be present prior to any installation or instantiation and must be re-obtained prior to each change in approach. All use of or modifications to AI technologies must go through formal change management in accordance with **Change Management Policy (IT-009-POL-EN)**.

4.5. AI ETHICAL ASSESSMENT

All AI projects or initiatives undertaken by Trinity must undergo an AI Ethical Assessment designed to reasonably identify and appropriately mitigate potential biases, risks, and adverse impacts on individuals, groups, or society as a whole ("inherent biases"). Data privacy, legal implications, and information security must be paramount in AI projects. Sensitive or personal data must be identified and approved by Data Owners prior to its use and processed/handled in compliance with applicable laws and regulations.

4.6. AI TRANSPARENCY

Transparency in the use of AI is essential to protecting the relationship between Trinity and its customers, stakeholders, and partners. The BPO is responsible for clearly communicating to users, customers, or stakeholders when AI is used to make a business decision and providing explanations of AI-driven decisions (when possible). Any installation or instantiation by Trinity of AI, inclusive of technologies that directly use AI in commercial/off the shelf (COTS) solutions, must be clearly cited and communicated to all impacted parties.

Continuous monitoring and evaluation of AI systems is essential to identify and rectify unintended consequences or biases that may emerge over time. The BPO responsible for the use of any AI is also required to initiate reviews of output from AI systems as frequently as required to reasonably reduce both (1) the risk to Trinity operations and objectives from inaccurate output, and (2) inherent biases. In no case shall this period of review exceed three (3) months.

5. EXCEPTIONS AND QUESTIONS

Questions about this document should be directed to the Document Owner. Exceptions to this document will be handled in accordance with the **Exception Management Policy (IRM-001-POL-EN)**.

6. ENFORCEMENT

Employees who violate this policy are subject to disciplinary action up to and including termination of employment. Trinity will take appropriate action to address violations by contractors, consultants, and similar labor providers. This may include termination of a contractual relationship, depending on the circumstances. Additional reporting or communication may take place in accordance with regulatory or contractual requirements.

7. RESPONSIBILITIES

The following roles and responsibilities are defined for this document. Each role must be one of the following:

- **Accountable (A):** An accountable role assigns work, reviews, and accepts it upon completion, and acts as the final point of authority. There may be one and only one role accountable for each task. If a role is accountable, it is also responsible, consulted, and informed.
- **Responsible (R):** A responsible role performs work to complete a task. There may be multiple roles responsible for each task. If a role is responsible, it is also consulted and informed.

- **Consulted (C):** A consulted role provides information, inputs, or guidance to a task. There may be multiple roles consulted for each task. If a role is consulted it is also informed.
- **Informed (I):** An informed role receives communications about the status of a task. There may be multiple roles informed for each task.

Action	BPO	CISO	CIO	CLO	E&C
Communicate the use of AI	A	C	C	C	C
Perform Intellectual Property reviews	C	C	C	A	C
Perform AI Technology Reviews	C	R	A	R	R
Perform AI Ethical Assessments	C	R	C	A	R
Review use of AI technologies	A	R	R	R	C
Perform AI accuracy reviews	A	I	C	I	

BPO = Business Process Owner CISO = Chief Information Security Officer CIO = Chief Information Officer
CLO = Chief Legal Officer E&C = Ethics & Compliance

8. References

The following documents are related to this policy and should be reviewed as necessary.

- Acceptable Use Policy (IRM-002-POL-EN)
- Change Management Policy (IT-009-POL-EN)
- Data Classification Policy (IRM-012-POL-EN)
- Enterprise Document Management Policy (DMS-001-POL-EN)
- Exception Management Policy (IRM-001-POL-EN)
- Global Logging Policy (IRM-010-POL-EN)
- Information Risk Management Definitions Standard (IRM-016-STD-EN)
- Information Security Policy (IRM-003-POL-EN)
- Vulnerability Management Policy (IRM-006-POL-EN)

9. Approval

Final approval by Brian Mork (Chief Information Security Officer) on 2025-03-03. All approvals are captured electronically in the Trinity Enterprise Document System.

10. History and Revision Log

Version	Author	Published Date	Summary of Changes
1.0.1	B. Mork	2025-03-03	Updated PII definition
1.0.0	B. Mork	2023-11-22	Initial release