



THINKTRENDS AI PLATFORM

Intelligent Infrastructure. Trusted by Design.

CUSTOMER DATA RESTRICTION & DATA SHARING POLICY

Customer Data Restrictions and Responsible Sharing

Document ID	TT-POL-CDR-001
Version	1.0
FedRAMP Package ID	FR2634659079
Classification	PUBLIC — CUSTOMER-FACING
Effective Date	October 20, 2026
Review Cycle	Each OCR cycle (quarterly) and at least annually; also on any change to the authorization boundary, the ThinkStack Data Inventory, or supported data categories
Document Owner	ISSO
Paramify Reference	Solution capability — Federal Customer Data Restrictions

PUBLIC — CUSTOMER-FACING | PUBLISHED VIA TRUST CENTER



TABLE OF CONTENTS

1. Purpose and Scope
2. Authorized Data and Impact Level
3. Unauthorized Information — Do Not Store or Transmit
4. Customer Responsibilities
5. ThinkTrends Responsibilities
6. Communication and Acknowledgement
7. Handling Unauthorized Information (Information Spill)



1. PURPOSE AND SCOPE

This policy defines what information customers and ThinkTrends personnel are **not authorized** to store in, upload to, or transmit through the ThinkTrends AI Platform (the ThinkStack platform); how that restriction is communicated to customers; and what happens when unauthorized information is found in the system.

It applies to every tenant in the FedRAMP 20x Class C authorization boundary and to all data paths into the platform: chat, agent building, document and knowledge-base upload, enterprise connectors, and the API.

It restates the responsibility recorded in the System Security Plan: **it is the responsibility of the Customer Admin to ensure that unauthorized information is not stored or transmitted within the platform.**

2. AUTHORIZED DATA AND IMPACT LEVEL

The platform is authorized under FedRAMP CR26 20x Class C. Customers may process data up to and including that level, limited to the categories enumerated in the ThinkStack Data Inventory.

3. UNAUTHORIZED INFORMATION — DO NOT STORE OR TRANSMIT

The following must not be entered into, uploaded to, or transmitted through the platform:

- Classified national security information, and any information carrying handling caveats the platform is not authorized for.
- Data whose sensitivity exceeds the platform's authorized impact level.
- Data categories not listed in the ThinkStack Data Inventory — including regulated categories the platform does not claim to support, such as PHI under HIPAA, PCI cardholder data, or Federal Tax Information.
- Credentials, private keys, tokens, or secrets for systems other than those a connector or integration is explicitly intended to reach.
- Personal information about individuals beyond what is necessary for the customer's authorized use case.
- Third-party proprietary or contractually restricted data the customer is not authorized to disclose to a cloud service.

4. CUSTOMER RESPONSIBILITIES

- The Customer Admin ensures their organization's users understand and follow this policy.
- The Customer Admin configures the tenant per the Secure Configuration Guide and restricts connectors and knowledge-base sources to authorized content.
- The customer notifies ThinkTrends promptly if unauthorized information is believed to have entered the platform.

5. THINKTRENDS RESPONSIBILITIES

- Publish this policy where customers can reach it (Trust Center) and reference it in onboarding materials and the customer agreement.



- Communicate the policy to each customer at onboarding, and re-communicate on any material change (new data-category support, boundary change, impact-level change).
- Provide configuration guidance (Secure Configuration Guide) that helps customers keep unauthorized data out.
- Monitor for indicators of unauthorized data and act on them.
- Treat confirmed unauthorized information in the system as an information spill (Section 7).

6. COMMUNICATION AND ACKNOWLEDGEMENT

- **Locations:** Trust Center (<https://trust.paramify.com/thinktrends>), onboarding packet, and customer-agreement reference.
- **Timing:** at onboarding; on any material change; and summarized in each OCR cycle.
- **Record:** the GRC Admin retains onboarding communications and change notifications.

7. HANDLING UNAUTHORIZED INFORMATION (INFORMATION SPILL)

Confirmed unauthorized information in the platform is handled as an information spill under the ThinkStack Incident Response Plan (Information Spillage Response). The Incident Response Admin opens a DFIR ticket, contains the spill (removing or isolating the data while preserving what is needed for investigation), eradicates the cause, and records a FedRAMP reportability determination on the ticket. Lessons learned feed the next review of this policy.

Version 1.0 — October 20, 2026. Prepared for FedRAMP CR26 20x Class C certification. © 2026 ThinkTrends AI Platform. All rights reserved.

— End of Document —