Five Practical Recommendations for More Secure AI

Technology Alliance for Statewide Initiatives

Brent Baker, CISSP, CISA, Security+

TASI Information Security Coordinator

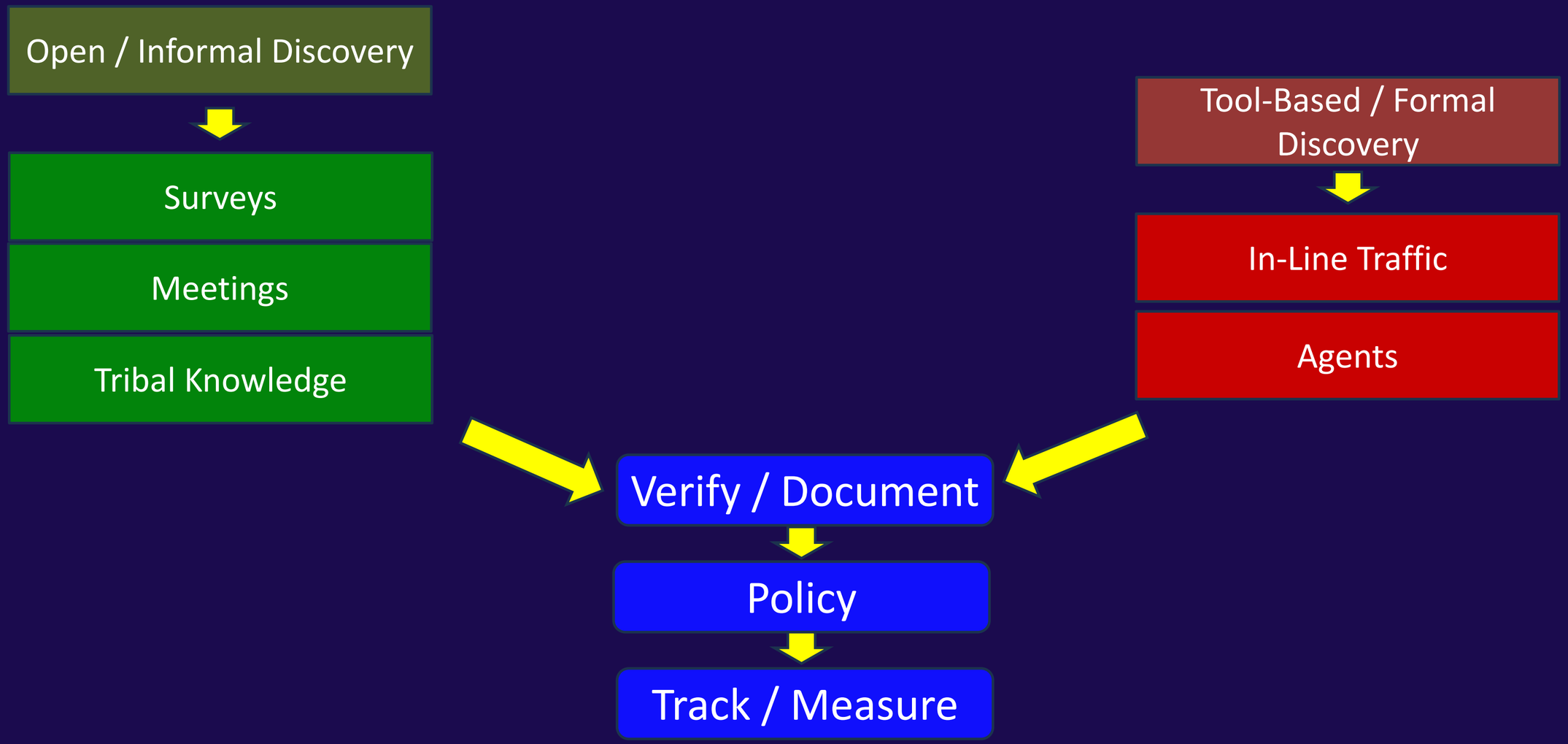
brent.baker@tasitx.org | 512.919.5371

Five Recommendations

1. Visibility
2. Develop an AI Policy
3. AI Vendor Selection & Management
4. PII Vigilance
5. Continuing Education

1. Visibility

Visibility: Two Approaches to AI Discovery



2. Develop an AI Policy

AI Policy: Necessary?

NO

Already covered

No support

Wait & see

YES

Unique & specific

Educate leadership

Entrenched, needs to be addressed

Examples of Policy Elements

1. Whitelist or blacklist approach?

2. Handling of personally identifiable info (PII)
   - Potentially more work – Is PII already defined in policy?

3. Usage guidelines & authorization
   - Addresses both generative & analytics/automation?

Examples of Policy Elements

4. Use of generative AI for public consumption:
    - Human-in-the-loop requirement
    - Disclosure / transparency

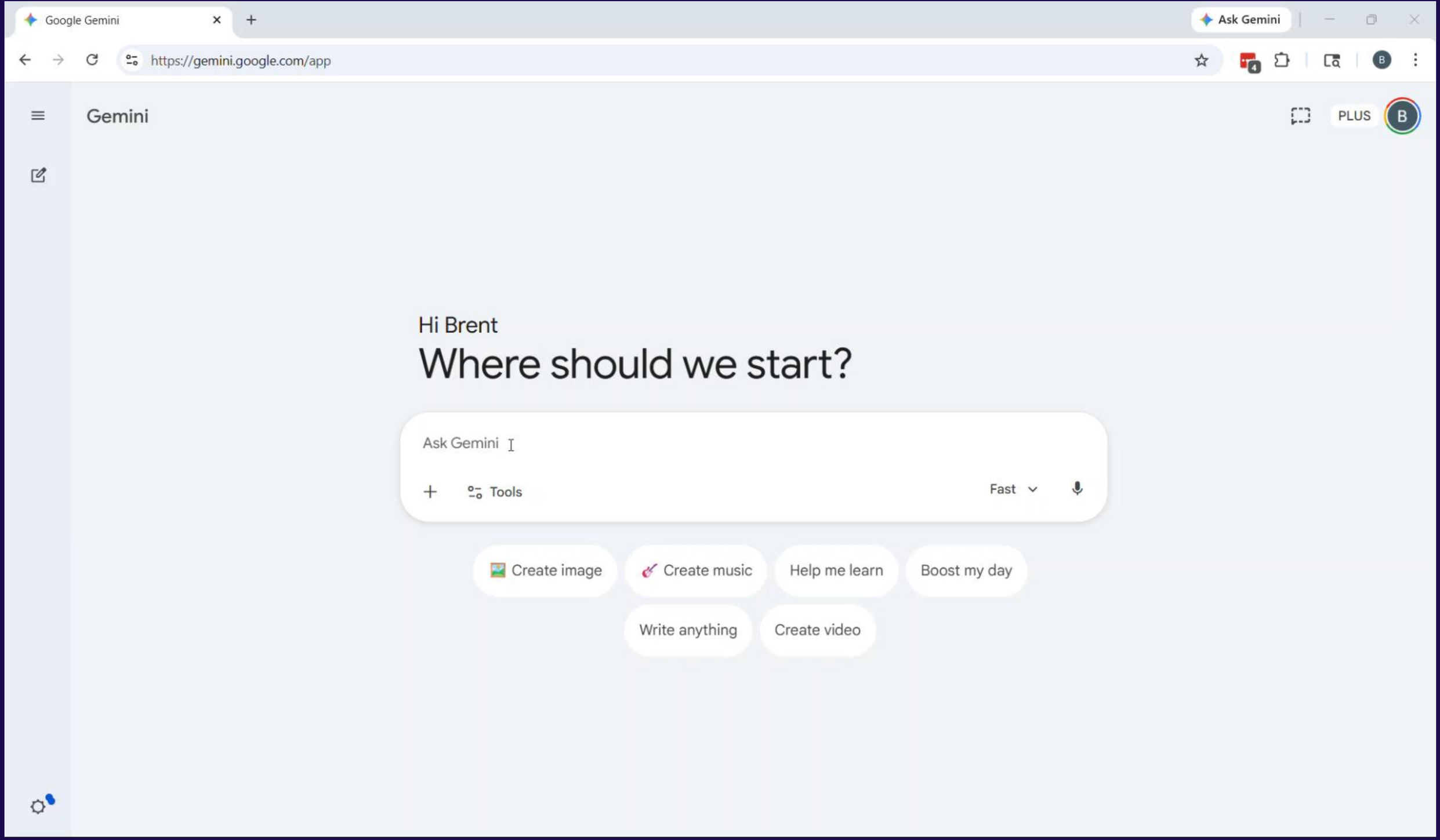
5. Handling of exceptions and policy updates

6. Education requirements

Policy Generation Prompt

Create an AI policy for Blue Bird ISD. The policy should be approximately 800 words. The policy must include the following:

1. Staff are not allowed to upload any personally identifiable information (PII) to AI systems without permission of the IT department. Include a definition of PII
2. Staff are only allowed to use these platforms for AI assistance: Magic School, school.ai, and Google Gemini
3. Best practices for justified use
4. Human verification of generative AI outputs
5. Best practices for disclosure and transparency of AI use
6. Staff must annually complete Texas HB3512 AI training


Google Gemini
Ask Gemini
https://gemini.google.com/app
Gemini
PLUS
B
Hi Brent
Where should we start?
Ask Gemini
Tools
Fast
Create image
Create music
Help me learn
Boost my day
Write anything
Create video

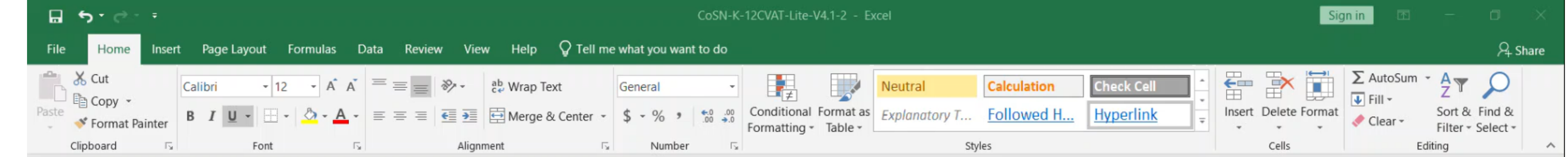
3. AI Vendor Selection & Management

3rd Party Vendor/Provider Vetting

CVATs (Community Vendor Assessment Tools)

- HECVAT (Higher Education CVAT)
- K-12CVAT (COSN, based on HECVAT, geared toward K-12)

K-12CVAT: K-12 Community Vendor Assessment Tool Lite-V4.1



A56 https://www.cosn.org/edtech-topics/cybersecurity/

CoSN
Leading Education Innovation

Shared Assessments Introduction

K-12 education environments are rapidly changing and the speed of cloud service adoption is increasing. Institutions looking for ways to do more with less see cloud services as a good way to save resources. As school systems deploy or identify cloud services, they must ensure the cloud services are appropriately assessed for managing the risks to the confidentiality, integrity and availability of sensitive institutional information and the PII of constituents. Many school systems have established a cloud security assessment methodology and resources to review cloud services for privacy and security controls. Other school systems don't have sufficient resources to assess their cloud services in this manner. On the vendor side, many cloud services providers spend significant time responding to the individualized security assessment requests made by K-12 school system customers, often answering similar questions repeatedly. Both the provider and consumer of cloud services are wasting precious time creating, responding, and reviewing such assessments.

The **CoSN K-12 Community Vendor Assessment Toolkit** (**CoSN K-12CVAT**), based off the Educause Higher Education Community Vendor Assessment Tool (or HECVAT), attempts to generalize K-12 education system information security and data protections and issues for consistency and ease of use. Some school systems may have specific issues that must be addressed in addition to the general questions sets provided in the toolkit. It is anticipated that the K-12CVAT will be revised over time to account for changes in services provisioning and the information security and data protection needs of K-12 education institutions.

The CoSN K-12 Community Vendor Assessment Toolkit:

- Helps K-12 school systems ensure that vendor services are appropriately assessed for security and privacy needs, including some that are unique to K-12 education
- Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs through vendor services without increasing risks
- Reduces the burden that service providers face in responding to requests for security assessments from higher education institutions

The CoSN K-12 Community Vendor Assessment Lite is a lightweight questionnaire used to a) expedite the process and b) begin to establish the process and build the muscle of assessing vendor risk.

Vendor / Service Provider Management

From ISACA AAISM 2.12

“When acquiring AI capabilities from external vendors, distinctions between providers and deployers become crucial for understanding responsibilities and managing risk effectively.

…An organization that leverages AI services from a provider should clearly understand and delineate the responsibilities shared between the provider and the organization.”

Shared Responsibility Model

For copyright reasons, the SRM graphics are not in this presentation. Information can be found at:

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/the-shared-responsibility-model-for-responsible-ai

4. PII Vigilance

Practical Case: PII Hiding

The SPED/Special Services department at your school district wants to collaborate with you (IT) to address their major time-consuming processes.

The goal is to streamline handling of IEPs, 504 plans, and similar PII-heavy document flows while providing in-depth analytical insights and reporting.

Practical Case: PII Hiding

You will work with an AI provider to develop your own LLM instance using their platform and processing. You will train the model with your own students' information, including assessments and existing reports.

You will subsequently rely on that trained model for your future advanced generative and analytical tasks.

Practical Case: PII Hiding

You want to follow the principle of “Privacy by design.” You will treat the acquired AI systems as potentially unsafe and will integrate PII protection throughout the process.

However, you also want to generate end products of quality reporting and materials specific to each and every student.

Hiding PII (names, SSNs, email, etc)

Non-Reversable

1. Masking (#######)
2. Redaction/removal
3. Hashing (one way), optional format preserving
4. Synthetic data generation, optional format preserving

Reversable

Tokenization:

-PII stored locally, token is swapped and later reversed
-Token not numerically related to source PII
-Can also follow format preserving encryption (FPE)

Can be handled in-line through automation

APIs / guardrails / strip / replace

Reversable example: On-prem / privacy filter (Open AI)

5. Continuing Education

Familiarity With AI Frameworks

Type	Examples
NIST AI RMF	Advisory in nature. The RMF is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.
ISO 42001	First international standard requiring certification and audits.
EU AI Act	First comprehensive regulation, similar to GPDR in reach.
OWASP AI Security Guide	Practical advice and references.

NIST AI Risk Management Framework

1. Advisory: Best practices
2. Emphasis on trustworthiness
3. Governance & transparency

Mastering AI Risk: NIST’s Risk Management Framework Explained. YouTube video, IBM technologies:

https://www.youtube.com/watch?v=0oeD2Wf25wY

Five Recommendations

1. Visibility
2. Develop an AI Policy
3. AI Vendor Selection & Management
4. PII Vigilance
5. Continuing Education

Thank you!

Technology Alliance for Statewide Initiatives

Brent Baker, CISSP, CISA, Security+

TASI Information Security Coordinator

brent.baker@tasitx.org | 512.919.5371

Technology Alliance for
Statewide Initiatives