MINNESOTA
IT SERVICES

Public Artificial Intelligence Services Security Standard

From the Office of the Chief Information Officer, State of Minnesota

Version: 1.0
Effective Date: 10/18/2023
Approval Signature: DocuSigned by: John Israel 9F634EA86D5A447... **Date**: 10/18/2023
John Israel, Chief Information Security Officer

Purpose

The purpose of this standard is to provide requirements and establish a framework for the responsible use of public web services enhanced by Artificial Intelligence (AI) (referred to in this standard as AI-enhanced services) for individual work tasks by State of Minnesota employees, volunteers, and contractors. It aims to guide employees, volunteers, and contractors on how to use publicly available AI-enhanced services such as Bing, Bard, and ChatGPT responsibly in a manner that:

- adheres to legal and regulatory requirements,
- balances confidence and skepticism,
- delivers value and benefits to Minnesotans, and
- secures protected information and data.

This document does not cover standards being developed to guide the acquisition, creation, or use of AI tools beyond individual work tasks like writing, editing, researching, or other duties that improve employee productivity. Information on those standards will be made available later.

Background

AI refers to the simulation of human intelligence processes by computer systems. If an application can independently perform tasks that would otherwise require human intelligence, such as understanding natural language, recognizing patterns, making decisions, or interpreting complex data, it likely uses AI.

AI-enhanced services have been used by organizations for many years. However, new large language model (LLM) AI-enhanced services that are on the Internet and embedded into tools such as Microsoft 365, and GitHub, create the need for new governance to use these tools responsibly. This standard refers primarily to these new services.

Publicly available AI-enhanced services can be very helpful for a variety of tasks. However, it is important to use these services responsibly and consider potential legal, practical, security, and privacy issues. The content produced by available AI-enhanced services should be consistently and skeptically reviewed by employees before they incorporate it into their work tasks.

People can input questions into publicly available AI-enhanced services. The responses mimic humans but because the AI-enhanced service is not a human subject matter expert it is at a risk of providing responses that are inaccurate or incomplete. Current AI-enhanced services do not understand questions, they generate word patterns that mimic content they have been trained to use.

When you submit data to an AI-enhanced service, it leaves a copy of the submitted data with the service. This may pose security and privacy risks. These risks are magnified if the AI-enhanced service automatically incorporates submitted data into responses shared with other users as part of the data they are trained to use.

This standard will use the terms Low, Moderate, and High data as defined in the Data Protection Categorization Standard. They have the following definitions:

- **Low**: Data that is defined by Minnesota Statutes Chapter 13 as "public" and is intended to be available to the public.
- **Moderate**: Data that does not meet the definition of Low or High. This includes but is not limited to system security information, not public names, not public addresses, not public phone numbers, and IP addresses.
- **High**: Data that is highly sensitive and/or protected by law or regulation. This includes but is not limited to: Protected Health Information (PHI), Social Security Administration (SSA) Data, Criminal Justice Information (CJI), Government-issued ID Numbers (e.g., Social Security Numbers, Driver's license numbers / State ID Card numbers, Passport Numbers), Federal Tax Information (FTI), (PCI) Account Data, Bank account numbers excluding State-owned bank account numbers.

Usage Standard

Allowed AI Services and Tools

- At this time, publicly available AI-enhanced services have only been approved for use with a Data Protection Categorization Level of Low.
- If you are uncertain whether a service or tool incorporates AI-enhanced services and/or whether you are allowed to use the service, contact the Secure Systems Engineering and Architecture Team for guidance (sse@state.mn.us). AI-enhanced services are reviewed and verified through a process that includes understanding the AI's training, ownership of data, and level of security.
- Any software or service where a third-party AI-enhanced service has access to State of Minnesota Moderate or High data needs to be reviewed and approved by the MNIT Secure Systems Engineering and Architecture Team before being used.

Prohibited Information

- Any data that is classified as Moderate or High by MNIT's Data Protection Categorization Standard must NOT be used in AI-enhanced services unless the AI-enhanced service has been approved through MNIT's vendor security risk and compliance process.
- At this time, AI-enhanced services must not be used in situations that can pose significant risks to the health, safety, or fundamental rights of persons. Such AI-enhanced services may be developed in the future but cannot be deployed until suitable governance processes are in place.
- Treat the information you are using in AI-enhanced services as if you were posting it on a public site and consider using AI-enhanced services as a starting point, as opposed to the final output, which poses less reputational, legal, and other risks.

Sample Use Cases

- At this time, commercially available AI-enhanced services may only be used for individual tasks that improve the way you work. Examples of acceptable use cases include:
  - Summarizing long documents that only contain public information.
  - Researching public topics where the resulting content can be verified by a subject matter expert (SME).
  - Generating draft documents that deal with public information.

  Examples of currently unacceptable use cases include:

  - Automatically responding to email messages without first reviewing content for accuracy and appropriateness.
  - Decision-making in situations where outcomes have not been verified by a subject matter expert. For instance, using AI-enhanced services to generate a list of possible hiring criteria for a new position, but not asking a human resources SME to review those criteria before posting the job.
  - Drafting a report that includes Moderate or High data.
- If there is uncertainty about how to use AI-enhanced services responsibly, please contact TAIGA for advice (taiga@state.mn.us).

Data Security

- State employees, volunteers, and contractors must ensure adequate security measures to protect Moderate or High data from unauthorized access, breaches, or misuse. This includes employing encryption, access controls, and regular security audits.
- State of Minnesota employees, volunteers, and contractors should recognize that commercial AI-enhanced services are for-profit tools designed to return shareholder value to the companies that create them. As such, they may provide value while simultaneously collecting data in a manner that benefits the AI-enhanced service but exploits users. These tools often provide limited value as they attempt to collect and sell not public, private, confidential, and restricted data.

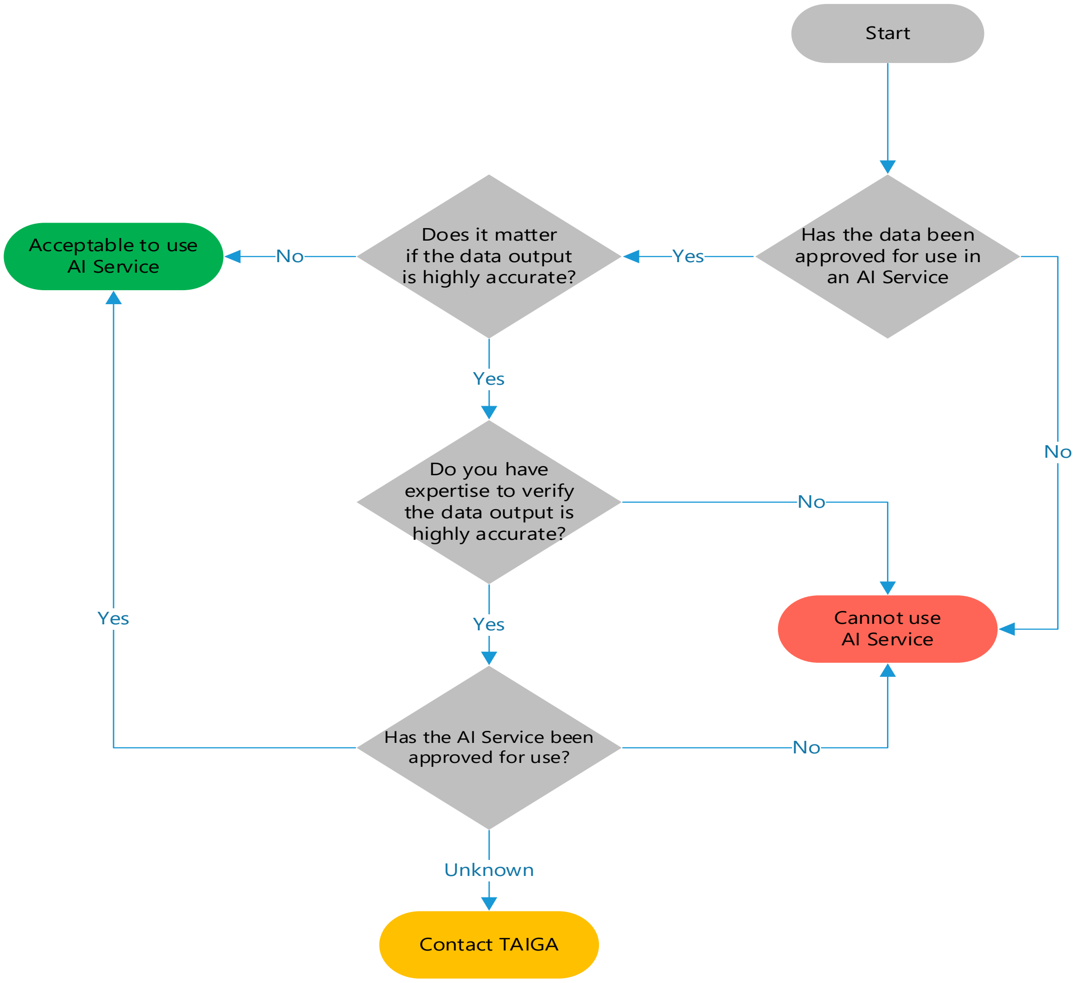
Compliance and Legal Considerations

- AI usage must comply with applicable laws, regulations, and industry standards. Legal and compliance teams should be consulted to ensure adherence to privacy, security, and other relevant regulations.
- Ensure that the output from AI-enhanced services is checked for facts, legality, and other responsible use concerns.
- AI-enhanced services should only be used to enhance human performance, not replace it. Do not use it as a substitute for your creativity, judgment, or expertise.

Training and Awareness

Regular training programs and awareness initiatives should be conducted to educate State of Minnesota employees, volunteers, and contractors about AI, its capabilities, limitations, and responsible use considerations. State employees, volunteers, and contractors are encouraged to report any concerns related to AI usage to the Transparent Artificial Intelligence Governance Alliance (TAIGA) (taiga@state.mn.us).

Approved Usage of AI-Enhanced Services Flow Chart


Start
Has the data been approved for use in an AI Service
Yes
No
Does it matter if the data output is highly accurate?
No
Yes
Acceptable to use AI Service
Do you have expertise to verify the data output is highly accurate?
No
Yes
Cannot use AI Service
Has the AI Service been approved for use?
Yes
No
Unknown
Contact TAIGA

Roles & Responsibilities

MNIT Secure Engineering and Architecture

- Maintain this document.

MNIT and Agency Based Office Staff

- Align usage of AI-enhanced services with this standard as dictated by state need.

Transparent Artificial Intelligence Governance Alliance (TAIGA)

- MNIT convened a group called the Transparent Artificial Intelligence Governance Alliance to work on AI governance issues including generative/publicly available tools, technology acquisition, and new development. TAIGA is developing processes to help catalog, evaluate, and implement technologies that incorporate artificial intelligence.

Applicability

This standard applies to all employees, volunteers, contractors, and third parties who develop, deploy, or utilize AI-enhanced services and applications within the Minnesota state government.

Related Information

- MNIT Services Data Protection Categorization Standard

History

Version	Description	Date
0.1	Initial draft	7/12/2023
0.2	Second draft to address feedback from TAIGA	8/3/2023
0.3	Third draft to incorporate reviewer comments	9/29/2023
1.0	Publish	10/18/2023

Contacts

Secure Systems Engineering and Architecture Team – sse@state.mn.us

Employees, volunteers, or contractors working on new applications that incorporate advanced AI and ML technologies should contact the Transparent Artificial Intelligence Governance Alliance (TAIGA) – taiga@state.mn.us – for more information on evolving governance work.