NORTH Dakota | Information Technology
Be Legendary.

Created: 04/17/2023
Revised: 11/17/2025
Reviewed: 11/17/2025

Artificial Intelligence Guideline

INTRODUCTION

PURPOSE

Outline best practices for secure, private, applicable, and ethical use of artificial intelligence (AI) technologies, so that state entities can feel comfortable exploring innovative ways to enhance the citizen experience and productivity. This guideline highlights common risks, challenges, and legal considerations when using this technology.

SCOPE

This guideline applies to all North Dakota executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e., campuses and agricultural and research centers. All other state agencies outside the scope of this policy are encouraged to adopt this guideline or use it to frame their own.

DEFINITIONS

Agentic Artificial Intelligence (AI Agent) – "Agentic" refers to the capability of an artificial intelligence system to operate with a degree of autonomy in pursuing assigned objectives. An AI Agent is a software-based system that uses artificial intelligence methods to perceive inputs, make context-aware decisions, and take actions—either digital or physical—toward achieving defined goals. AI Agents may perform tasks on behalf of individuals or organizations, can interact with other systems or users, and may adapt their behavior based on data, rules, or learned patterns.

Artificial Intelligence (AI) – A field in computer science that focuses on independent decisions based on supervised and unsupervised learning.

Machine Learning (ML) – A subfield of AI that focuses on the development of algorithms and statistical models to make independent decisions, but still needs humans to guide and correct inaccurate information. ML is the most common type of AI.

Large Language Models (LLMs) – A type of AI that has been trained on large amounts of text and datasets to understand existing content and generate original content.

Deep Learning – A subfield of machine learning that focuses on algorithms that adaptively

learn from data without instruction or labeling. Also referred to as "unsupervised learning."

Examples: self-driving cars, facial recognition, ChatGPT et al.

Generative AI – A type of AI that uses machine learning to generate new outputs based on training data. Generative AI algorithms can produce brand new content in the form of images, text, audio, code, or synthetic data.

Business Owner – an entity's senior or executive team member who is responsible for the security and privacy interests of organizational systems and supporting mission and business functions.

Data Owner – individual/individuals responsible and accountable for data assets.

Data Steward – individual/individuals with assigned responsibility for the direct operational-level management of data.

GUIDELINE

North Dakota state government branches, agencies, and entities are responsible for developing and administering policies, standards, and guidelines to protect the confidentiality, integrity, and/or availability of state data. This guideline was developed to supplement the Artificial Intelligence Policy, to prevent the misuse of AI and ML technologies, minimize security and privacy risk, and reduce potential exposure of sensitive organizational or regulatory data.

Additional AI education and resources can be found at the Artificial Intelligence page of TeamNDConnect You will need state issued credentials to access these materials.

SECURITY AND PRIVACY

AI/ML systems are designed to adapt to data input and output, putting privacy at risk when sensitive data is utilized as input. Data entered in public AI/ML services is not secure and not protected from unauthorized access. These public AI/ML services may incorporate input into their learning model, which can expose data as output to other individuals.

- If the data/business owner is evaluating AI for a business use case, submit an Initiative Intake Request via the NDIT Self-Service Portal.
- The State of North Dakota will consult the National Institute of Standards and Technology (NIST) Special Publication (SP) 1270 Towards a Standard for Identifying and Managing Bias in Artificial Intelligence, NIST AI 100-1 Artificial Intelligence Risk Management Framework, and other regulatory frameworks for guidance on AI best practices.

- Use of state-issued email address for the creation of user-ids for free and public AI resources (i.e. ChatGPT) is not recommended. However, if necessary, it is permitted if you use a unique password.
    - Personally managed accounts created with personal email usernames are recommended for exploratory use of public services while use of state-issued credentials is recommended for enterprise AI solutions.
    - Use of state issued email as the username for 3rd party accounts, used for public services, may cause confusion or technical issues down the road. For example, if the State pursues an enterprise offering on the same platform and connects it to the State single sign on solution, one might end up with two similar logins for that platform. This is because, there is typically a tie-in to managed State accounts, which uses state issued email addresses as part of the login by default.

BIAS AND ACCURACY

AI/ML technology services are only as accurate as their datasets. All data has some level of bias. AI applications will reflect any bias present in the data on which it is trained, as AI/ML technologies do not understand your data. As with any use of data, it is important to have a thorough understanding of your data quality, if your data is a representative sample of the population it represents, and what any deficiencies might mean for the usefulness of your analysis.

Data can also be compromised by individuals with malicious intent and result in intentionally biased data, tailored propaganda, or inaccurate results. Output from AI can also result in unintentional bias.

- Accuracy of output should be evaluated prior to use, and evaluated regularly thereafter.
- Users should always use trusted and reliable sources for confirming information results that come from AI/ML. Decisions made using biased analysis might have unintended consequences for the populations we serve.
- Approved vendor or internal AI/ML services require periodic quality assurance checks to ensure AI-driven outcomes are accurate.
- Verify accuracy prior to use, and exclude moderate-risk and high-risk data following the Data Classification Policy.

Approved AI or ML enhancement products may include browser plugins, mobile applications, websites, etc.

With popularity of new AI/ML technologies, threat actors have created legitimate-looking browser plugins, mobile applications, and other technologies that are used for malicious intent.

BUSINESS USE CASES

- Content Curation: Drafting, refining, editing, reviewing, and creating stylized writing.
    - Emails
    - Presentations
    - Memos
    - Marketing
- Text Summarization
- Preliminary Research
- Chatbot: Customer Service and Support
- Programming/Code Generation
- Automation
- Media Creation: Audio, Video, and Images
- Prediction and other analytics applications

EXAMPLES OF ACCEPTABLE USE

The following are some examples of acceptable use and non-acceptable use of publicly available or privately managed common AI tools. The key is to understand who is managing your user identity and be aware of the sensitivity of data you may be exposing and to follow standard password management practices.

The value of acquiring enterprise versions of such tools is to allow for acceptable use in more sensitive use cases. Enterprise versions of tools provide more safeguards to control of the flow of data in and out of these models. This allows for use of the same tools for internal scenarios, such as system configuration, internal policies, and other information that is not shared outside the organization or certain teams.

How do I know if I'm using an enterprise version of a tool? Here are a few tips for helping you determine this:

1. Typically, if you need to self-register to use the tool, this usually means the State is not managing this user account. If it was a managed account, you'd be able to sign in the State Credentials without having to register and create password. This is the same account used to sign into your computer.

    a. Such accounts are managed by the vendor and used to keep your search history and preferences tied to your account for useability purposes. There is no tie to any other accounts, even if you reuse the same email/username.

2. When using a public or privately managed service, it does not ensure the data you input (questions your ask) or the responses you receive are private or secure. It's comparable to signing into google, then using the search engine.

The following examples highlight the differences of using some popular tools vs. an enterprise solution built on the same technology.

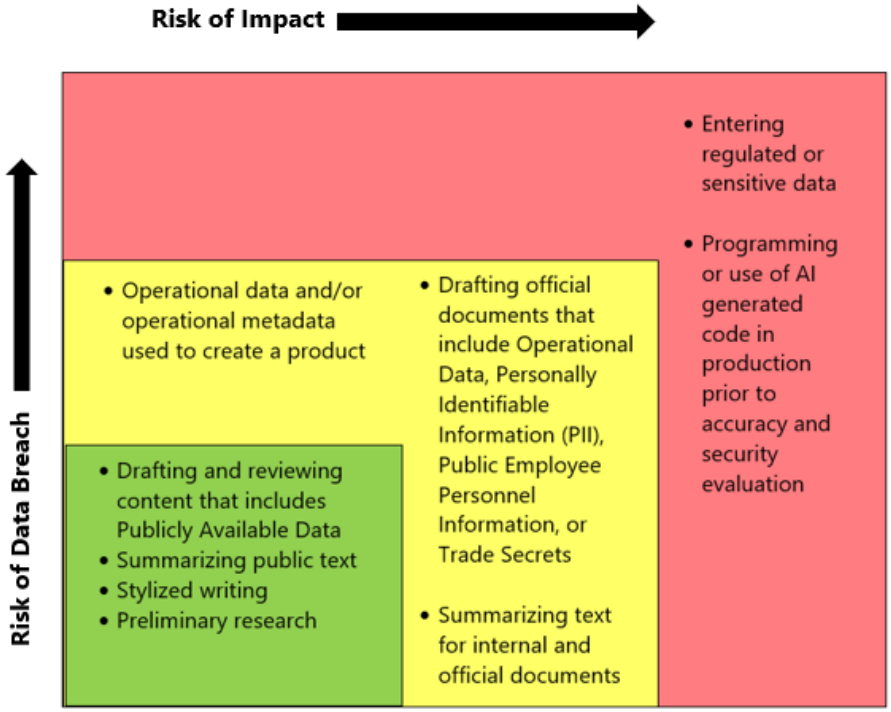
Example Scenario: Creating a policy or process for your organization

Available Tool: Publicly available version of ChatGPT by OpenAI

Considerations: A tool readily available, but utmost care is required when sharing data

Acceptable Use	Not Acceptable Use
• Register an account with tool/service using my personal or my state-issue email address **using a different, unique password**.	• Register an account with tool/service using my personal email or my state-issued email address **reusing an existing password** from any of my other accounts I manage.
• Ask the tool to summarize to gather information about a topic using information that **doesn't include any internal or sensitive information** which would be considered inappropriate to publish publicly.	• Ask the tool to summarize to gather information about a topic that **includes internal or sensitive information.**

Internal or sensitive information refers to data outlined in the "Data Classification Policy" as medium and high-risk data.



AI Risk Matrix

*The AI Risk Matrix and use of data following the Data Classification Policy is applicable to most AI. Use of data within approved AI Enterprise solutions is dependent on the results of a risk assessment and impact analysis conducted by the NDIT Governance, Risk, and Compliance (GRC) Team, with Executive Leadership Team (ELT) approval.

- Users and agencies may also check with their Technology Business Partner (TBP) and Information Security Officer (ISO) if unsure on appropriate business use cases.

Questions on AI can also be sent to **aiquestions@nd.gov**.

TRAINING RESOURCES

- NDIT shall provide self-paced AI training through curated materials on the State intranet, training sessions via the NDIT One-Stop Shop, and the cybersecurity education platform.

- NDIT shall offer live AI training sessions via MS Teams or in-person, scheduled through a Service Now request to the Technology Outreach Team.

REVISION HISTORY

Date	Authored	Approved by	Version	Description of Change
4/17/2023	NDIT AI Team	Josh Kadrmas	0.5	Initial Draft Created
8/21/2023	NDIT AI Team	Josh Kadrmas	0.6	Initial Draft
9/11/2023	NDIT AI Team	Josh Kadrmas	0.7	Initial Draft Revisions
12/11/2023	NDIT AI Team	Jason Anderson	0.8	Draft revision
1/3/2024	NDIT AI Team	Jason Anderson	0.9	Draft revision
1/26/2024	NDIT AI Team	Jason Anderson	0.10	Draft revision
1/30/2024	NDIT AI Team	Jason Anderson	1.0	Final version
12/10/2024	NDIT GRT	Governance Review Team	1.1	Annual Review
11/17/2025	NDIT GRT	Governance Review Team	1.2	Annual Revisions

APPENDIX. SUPPLEMENTAL GUIDANCE

RESOURCES

- National Artificial Intelligence Initiative: The National Artificial Intelligence Initiative (NAII) National Artificial Intelligence Initiative
- National Institute of Standards and Technology (NIST): Artificial Intelligence Risk Management Framework (AI RMF 1.0)
- Microsoft 365 Definitions of AI: Unleash your productivity with AI and Microsoft 365 Copilot - Microsoft Support
- Gartner: Gartner Information Technology Glossary
- NDIT Artificial Intelligence Policy: ndit.nd.gov/governance/policies
- AI Supplementary Guidance: ndgov.sharepoint.com/sites/TeamND/SitePages/Artificial-Intelligence

FAQ

- Is artificial Intelligence a threat to security?
  - Just like any new technology, AI can be used in a positive and negative manner and is driven by the intent of the human using the technology. AI has powerful capabilities to help increase an organization's efficiencies but must also be properly vetted and assessed for risk prior to its use.

- Is artificial intelligence a threat to privacy?
  - AI is a threat to privacy only if the information provided as input into the data model is not publicly available data or prepared open record data. Public AI prompts should be generic and not include sensitive or regulated data.

- What should I do if sensitive or regulated information disclosure has occurred while using Generative AI (public sources, i.e. ChatGPT)?
  - Notify your data steward or manager and submit a ServiceNow incident.

- Why should I be concerned about the data or information I put in online AI tools like ChatGPT? What happens to that data or information?
  - By default, models like ChatGPT use any data you provide to train and improve their models. Even if you disable this by disabling the chat history setting, the data may be still stored for a set amount of time. There should be no expectation to security and privacy if sensitive information is provided within platforms like ChatGPT.

- How can I determine what AI/ML technologies are approved for use by NDIT?
  - Contact your Technology Business Partner (formerly Customer Success Manager) or Information Security Officer. If you are not sure if one is assigned to your agency, contact the NDIT Service Desk at (701) 328-4470 or submit a NDIT Initiative Intake via ServiceNow.

- What information is needed by me and my agency if there's a business desire to incorporate AI into our business using AI technology?
  - Evaluation of AI technologies can be requested through the NDIT Initiative Intake request. The following items must be included in the request:
    - What are you trying to solve for?
    - What is the current pain point and why/how can AI deployment solve the problem?
    - Provide insight on impact of adopting AI and how responsible and ethical use of AI would be accomplished.

- What can cause my data to be "biased"? What can I do to ensure my analysis is as free from bias as possible?
    - Data represent a subset of the truth, taken at a particular point in time, so all data have some level of bias. When you use an existing AI tool, understand there might be intentional or unintentional bias in the data used to train that model that you may or may not know about. Keep this in mind when you consider the output of such a tool.
    - When creating a model using your own data, consider how the data sets you are using were collected, and how well that data is able to represent truth. There are tools or techniques that can be used to help you determine if your own models contain biases.
- What are some examples of tasks or projects for which I should not use AI?
    - **Decision-Making:** Tasks that requite decision making should still be completed using human intelligence.
    - **Creative work:** Outstanding questions about copywrite law can make using AI for creative aspects of official work problematic.
    - **Tasks that require a high amount of emotional interaction:** AI is not great with tasks that require human connection or empathy. For example, a doctor might use AI to help with a diagnosis, but would not use AI to discuss a diagnosis with a patient.
- What are some examples of tasks or projects where I should consider the use of AI?
    - **Chatbots and Virtual Assistants:** AI is great for tasks like translation, proof-reading, first drafts of communications, summarizing text, and organizing visual media.
    - **Sentiment Analysis:** AI can provide some understanding on general attitudes toward topics.
    - **Fraud/Malicious Detection:** AI systems can help people detect fraud, misuse, or malicious intent quickly. For example NDIT Security uses tools to monitor and analyze network traffic in real-time, with the goal of detecting suspicious activity immediately.
    - **Predictive Analytics:** AI can take data from the past to assist in projecting what might happen in the future.
- Is there an artificial intelligence policy?
    - Yes. It is found on the NDIT website under the policy section.
- Who can I contact if I have questions about AI
    - aiquestions@nd.gov