Generative Artificial Intelligence (AI) Usage Standard

Definition

For this cybersecurity standard, "AI" refers to software algorithms that generate original content, such as artwork, music, or text, based on input parameters or data, and excludes other forms of Natural Language Processing and Machine Learning.

Objective

Emerging generative AI tools including ChatGPT, AWS (Amazon Web Services) Bedrock, and Google Bard can serve as powerful assets in supporting the work of organizations and individuals, yet they introduce unique challenges and ethical dilemmas. Use of AI tools could impact the cybersecurity of The University of Texas at Dallas (UT Dallas) in both positive and negative ways, suggesting the need for clear governance and documentation of expectations. Thus, this standard delineates acceptable and unacceptable uses for generative AI tools and must be referenced when evaluating how best to manage generative AI tools within UT Dallas.

Scope

This standard applies to all UT Dallas employees performing official work duties. This standard is not intended to govern academic conduct, plagiarism, or the impact of generative AI tools in the context of students in academic settings.

1. Acceptable Use

1.1 Data

1.1.1 Users are allowed to input Public Data into generative AI tools.

1.1.2 Users should be aware that the integrity of University Data may be undermined if processed by AI tools.

1.1.3 AI tools may be used in the performance of research activities not classified as containing Confidential Data; Confidential Data may not be uploaded to AI tools unless such tool is provided by UT Dallas. Class instructors may use AI for developing instructional materials, provided that Confidential Data is not uploaded to AI tools unless the tool is provided by UT Dallas.

1.1.4 Users should be aware that output from AI tools is not guaranteed to be accurate, as AI learning models may produce output that is subject to biases, inaccuracies, or which may infringe copyright laws.

1.1.5 UT Dallas employees performing official work duties are accountable for deliberate and/or unintentional misuse of AI-generated content, dissemination of misinformation from AI-generated data, or exposure of Confidential Data.

1.2 Private AI

1.2.1 When using AI tools to support official UT Dallas job duties, it is recommended that users employ AI tools offered by UT Dallas, rather than obtaining personal access to public or vended AI platforms which are not pre-approved for UT Dallas employees to work with.

1.2.2 Users must adhere to contract terms and license agreements associated with AI tools offered by UT Dallas to support the work of employees.

1.2.3 Datasets accessed through AI tools must be used in accordance with applicable licenses.

1.3 Third-Party Software-as-a-Service (SaaS)

1.3.1 Users may operate generative AI Software-as-a-Service (SaaS) tools officially offered by UT Dallas. AI tools approved for employee usage are offered through the Office of Information Technology (OIT).

1.3.2 At the time of this writing, OIT offers the following AI tools: 1. GPT access within Microsoft Azure; 2. Bedrock within AWS. OIT can help UT Dallas employees by discussing needs and providing guidelines for safe handling of University Data when interacting with AI tools.

1.3.3 Future procurement of third-party hosted solutions which offer AI features must be reviewed by the Office of Contract Administration (OCA).

1.4 Use of Already-Contracted Services

1.4.1 Prior to seeking additional AI service providers, employees must first consider the feasibility of existing service offerings contracted by UT Dallas, in consultation with OIT.

1.5 Examples of Regulated Data

1.5.1 Data may be subject to regulatory and/or contractual requirements that prohibit input of such data into AI tools, regardless of whether UT Dallas has approved and offered the AI tool to support general productivity of employee work. The University Attorney is responsible for reviewing and approving specific scenarios where regulated data may, or may not, be allowed to be used with AI tools. Examples of regulated information that should not be input into AI tools include, but are not limited to:

1.5.1.2 Health Insurance Portability and Accountability Act (HIPAA) regulated data.

1.5.1.1 Family Educational Rights and Privacy Act (FERPA) regulated data.

2. Prohibited Use

2.1 Data

2.1.1 UT Dallas employees may have access to publicly available AI tools which they choose to utilize for personal reasons. Such tools, not officially offered by UT Dallas, may not be used in the performance of job duties, and may not receive Confidential Data, as defined by UTDBP3096 - Information Security and Acceptable Use Policy.

2.1.2 Publicly available AI tools not officially offered by UT Dallas should not be used to produce data output that would then be classified as official University Data. Examples include generating data for non-public research, academic work, or instructional materials.

2.2 Law

2.2.1 Actions performed with AI tools during the performance of job duties cannot violate any applicable state or federal law, UT Dallas policy, or UT System policy.

2.3 Contract Offboarding

2.3.1 When UT Dallas contracts for AI tools, it is preferable to include specific and accepted training tools to familiarize employees with responsible use.

2.3.2 When UT Dallas contracts for AI tools, it is preferrable to include specific and acceptable methods of data destruction at the end of the business arrangement that ensure the protection of University Data.

2.4 Automation

2.4.1 UT Dallas employees must thoughtfully approach opportunities where AI tools are being considered to fully automate current business processes and functions.

2.4.1.1 Such process changes must consider the impact on current employees.

2.4.1.2 Applicable laws, contracts, and policies.

2.4.1.3 Potential for automation to produce outcomes that would be undesirable and unlikely to be produced by humans performing the process manually.

3. Use of Results

3.1 Audit Logging

3.1.1 It is preferrable that AI tools produce transaction logs and/or offer sufficient records to document decisions that were made by the tools.

3.1.2 Users are reminded that University-owned networks and computing devices are subject to various forms of monitoring by organizational units, such as ISO and OIT, for the purpose of achieving intended performance and security protections.

3.2 Oversight

3.2.1 It is preferable that impactful decisions made by AI tools be reviewed and approved by human employees with sufficient knowledge of the relevant processes, stakeholders, and other consideration, thus promoting the reasonableness and soundness of decisions.

4. Ethical Use of Generative AI

4.1. Human Rights and Privacy

4.1.1 Generative AI tools should be used in a manner that upholds and respects human rights and privacy. Content generated should not be discriminatory, harassing, or defamatory.

4.2. Bias and Discrimination

4.2.1 Users must understand that AI learning models receive incomplete or biased data as inputs, and as a result, may output imperfect data. UT Dallas employees should strive to avoid perpetuating biases through AI. This includes biases related to race, gender, age, and other protected characteristics.

4.3. Transparency and Accountability

4.3.1 Users of AI tools are encouraged to be transparent about the use of AI-generated content and will be held responsible for any content they create with AI and subsequently portray as their own work.

4.4. Harm to Individuals or Groups

4.4.1 Content generated through AI should not cause harm to individuals, groups, or communities, and should comply with applicable laws and regulations.

4.5. Positive and Constructive Content

4.5.1 Users should strive to generate positive, constructive content aligned with the University's values, mission, and policy.

5. Incident Response and Reporting

5.1 Please contact infosecurity@utdallas.edu with questions, comments, and/or concerns.

6. Periodic Review and Update

6.1 This documented standard is subject to periodic review and updates, if necessary, to ensure it remains aligned with evolving technology and policies. This standard is published by the Information Security Office (ISO) in partnership with the Office of Information Technology (OIT).

8. Exemptions

8.1 In the event that an employee of UT Dallas believe they might not be able to achieve full compliance with this standards, please contact infosecurity@utdallas.edu to submit an exemption request which will be reviewed and then approved or denied by the Chief Information Security Officer (CISO).

8.1.1 Denied exemption requests may be appealed to the UTD President for a final decision.

9. Conclusion

9.1 AI tools can enhance teaching, learning, and research at the University of Texas at Dallas, but it is important to approach its use with caution and responsibility. By adhering to this standard, we ensure that the use of AI supports the University's mission while minimizing risk.

Revisions

Date:	Name:	Changes / Notes:
October 13, 2023	Silas Vieira	Completed draft review and published as final