Cybersecurity Policy Templates

Artificial Intelligence Standard

(Last Updated April 2025)

Scope

This policy applies to all <Company Name> employees and affiliates.

Safeguards

I. Introduction.

YourCompanyName is committed to full compliance with applicable laws related to the use of artificial intelligence in the countries in which YourCompanyName provides products and services. Additionally, YourCompanyName is committed to the ethical use of artificial intelligence. This Artificial Intelligence Use Policy ("Policy") outlines YourCompanyName's requirements with respect to the adoption of all forms of artificial intelligence at YourCompanyName. Such artificial intelligence adoption includes use for business efficiencies, operations, and inclusion in YourCompanyName's products and services.

This Policy is applicable to all YourCompanyName directors, officers, board members, employees, contractors, representatives, affiliates, agents, and any person or entity performing services for or on behalf of YourCompanyName. The ResponsibleCorporateOfficer at YourCompanyName is responsible for the enforcement of this Policy.

II. Definitions.

"Artificial intelligence" or "AI" means the use of machine learning technology, software, automation, and algorithms to perform tasks and make rules or predictions based on existing datasets and instructions.

"Artificial Intelligence Committee" or "AI Committee" is an internal YourCompanyName committee tasked with reviewing and approving uses of AI at YourCompanyName.

"Artificial intelligence system" or "AI system" means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

"Closed AI system" means an AI system where the input provided by one user is used to train the AI model. Input data from the user is isolated from other users, and the data is considered more secure.

"Embedded AI Tools" means AI tools embedded in existing software tools approved and used at YourCompanyName and which do not require approval for use from the AI Committee.

"Government" means the government of a country or subdivision thereof.

"Government Entity" means any entity controlled by a government in whole or part. This includes Government-owned or controlled (whether whole or partial ownership or control) commercial enterprises, institutions, agencies, departments, instrumentalities, and other public entities, including research institutions and universities.

"Government Official" means any officer or employee of a Government Entity, an official of a political party, a candidate for political office, officers and employees of non-governmental international organizations, and any person with responsibility to allocate or influence expenditures of Government funds. This includes data scientists and researchers who are employed by a government or a Government Entity. Employees at government organizations are considered Government Officials regardless of title or position.

"Non-public YourCompanyName data" means any information that, if disclosed, could violate the privacy of individuals, government regulations or statutes, could jeopardize the financial state of YourCompanyName, could injure its reputation, or could reduce its competitive advantage.

"Open AI system" means an AI system where the input provided by all users is used to train the AI model. Input data from all users is not private and may be revealed to other users.

"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household.

"YourCompanyName Representatives" means all YourCompanyName directors, officers, board members, employees, contractors, representatives, resellers and sub-

resellers, distributors and sub-distributors, affiliates, agents, and any person or entity performing services for or on behalf of YourCompanyName.

III. Guiding Principles.

The intent of this Policy is to provide general guidance on the use of AI at YourCompanyName so that YourCompanyName can leverage the use of AI as a tool while ensuring it continues to meet legal obligations and act in an ethical manner. The use of AI at YourCompanyName should never compromise YourCompanyName's core values or introduce undue risk to the organization. Rather, the use of AI at YourCompanyName should be focused on improving business efficiencies and enhancing YourCompanyName's ability to fulfill its mission.

It is important to remember that the YourCompanyName is a global organization. The YourCompanyName has entities and staff globally and provides its products and services to customers globally as well. Accordingly, this Policy provides overarching guidance based on global standards for the use of AI. YourCompanyName Representatives should be cognizant when using AI at YourCompanyName that they think about the global impact of their decision to use AI, as the use of AI in some countries may not be permitted in others.

This Policy is not intended to address every use of AI at YourCompanyName by a YourCompanyName Representative. There are certain business departments and functions at YourCompanyName that bear more considerations and potential risks. Before using any AI at YourCompanyName—whether for personal business tasks such as writing an email or more complex business processes such as analyzing datasets - you should consult with your manager and seek guidance. Also, please see Prohibited Uses in Section IV below for situations in which AI may not be used at YourCompanyName, and High-Risk Use of AI Systems in Section VI below for situations in which extreme caution is required when considering using AI.

In addition, there are certain Embedded AI Tools used in existing approved YourCompanyName software that do not require additional approval for use. For example, the use of Microsoft Word in which Microsoft Word has embedded an AI tool to check spelling or grammar. The use of Embedded AI Tools in approved software at YourCompanyName is permitted, provided those software tools are aligned with previous general business uses. A list of existing software tools with Embedded AI Tools that are approved at YourCompanyName can be found here [INSERT LINK].

When third-party software, services, or contractors are utilized or employed, any AI usage by software used by these parties or services must be noted and evaluated carefully. Contracted services that utilize AI technology should be considered in the same light as individual AI usage. Consult with the Legal Department about the inclusion of an AI-specific clause in any vendor or contractor agreements.

The following principles must be followed when considering using an AI system at YourCompanyName:

- The use of an AI system should primarily focus on completing departmental goals as directed by company leadership. Except for the use of an Embedded AI Tool in a software system approved for use at YourCompanyName, any use of a new AI System at YourCompanyName must be approved by the AI Committee. Please see the Standard Operating Procedure here [INSERT LINK] for the process for getting an AI system approved. Also, see General AI Use Standards and Use Approval in Section IV below.

- Individuals using an AI system must have expertise in the subject matter for which the AI is used. AI is to be utilized as a tool and is not a substitute for expertise. For example, if using AI for coding, the individual deploying the AI must have expertise in coding.

- All AI-generated content (writing, datasets, graphs, pictures, etc.) must be thoroughly reviewed by an individual with expertise to evaluate such content for accuracy as well as general proofing and editing. AI-generated content should be viewed as a starting point, not the finished product. Like any content at YourCompanyName, AI-generated content should conform to the look and feel of the YourCompanyName brand and voice.

- Any use of an AI system must have clear objectives for the AI use as a tool and business-accepted data sets from which the AI draws. If the data sets that the AI is using are not accurate, then the information AI provides will not be accurate.

- AI systems are trained on data that may contain inherent bias. Users of these systems are responsible for reviewing any AI-produced content for bias and correcting it as necessary.

- Non-public YourCompanyName information must never be put into an open AI system.

- YourCompanyName Representatives must document all AI systems they are utilizing and for what functions. Tracking the use of AI is not optional and is part of your job. Documentation of specific AI Embedded Tools in an approved existing software tool when using that tool as intended is not required. Discuss the process for tracking the use of AI systems with your department head.

- The use of an AI system must be documented to capture institutional knowledge. For example, if AI is used to create code and included in a larger section of code, there must be documentation as to which code section is AI-derived and who reviewed it.

- The use of an AI system must meet any terms of use or contractual limitations. Contractual restrictions or terms of use may restrict YourCompanyName's use of an AI system that would otherwise be legally compliant and ethically sound. For example, an AI system's terms of use may require the use of certain disclaimers in certain use situations or prohibit the use of the AI system to do certain tasks. YourCompanyName Representatives should have all terms or use or contracts for AI systems reviewed by the Legal Department to ensure compliance with contractual obligations in using an AI system.

- Approval of an AI system does not eliminate the need for other internal approvals required at YourCompanyName for the use of technology, such as a security review, privacy review, cost review and spend approval, legal review, human resources review, etc. An AI system should go through the same review and approval process as other software or services at YourCompanyName. You should also ensure within your business unit that your business leader is aware of the use of the AI system and has approved any use of the AI system, particularly for AI-generated content that will be relayed externally.

IV. Prohibited Uses.

There are certain uses of AI that are prohibited. Unless otherwise approved by the AI committee and respective department heads, YourCompanyName Representatives are prohibited from using AI systems for any of the following activities at any time:

- Conducting political lobbying activities is prohibited. Lobbying is defined as any action aimed at influencing a Government, Government Official, or Government Entity for any reason.

- Using AI systems to identify or categorize students, candidates, employees, contractors, or other affiliated entities based on protected class status is prohibited.

- Entering trade secrets, confidential information, or personal data about any individual into an open AI system.

- Entering any sensitive information about an individual into any AI system. "Sensitive information" includes medical, financial, political affiliation, racial or ethnic origin, religious beliefs, gender, sexual orientation, disability status, or any other part of a person's life someone would want to keep private.

- Using an AI system to obtain legal advice, including, but not limited to, creating policies for internal use or to provide to third parties.

- Creating intellectual property that YourCompanyName desires to register and/or holds significant value to the organization.

V. Ethical Guidelines.

YourCompanyName desires to act in an ethical manner when using AI. Accordingly, there may be uses of AI that are legally permissible but which do not meet ethical requirements. Any use of an AI system at YourCompanyName should conform to the following ethical guidelines:

- **Informed Consent:** Prior to inputting personal information into a closed AI system, ensure that you have obtained informed consent from the individual(s) whose personal information will be inputted.

- **Integrity in Use**: All users of AI systems should be honest about how AI helped in getting the work done. Even if using an AI system approved by the AI Committee for an approved use, you should ensure your manager or the department requesting a task for which you are using an AI system is aware of your use of the AI system. Do not pass off AI-generated work as done by you solely. Additionally, you should ask permission if you desire to use an AI system tool to complete a task. For example, you should ask your manager and HR representative if you may use an AI system to assist in writing a performance evaluation.

- **Appropriate Content**: Do not use company time or resources to generate content using an AI system that would be considered illegal, inappropriate, harmful to YourCompanyName's brand or reputation, or disrespectful to others.

- **Unauthorized Use:** Do not use company time or resources to generate content using an AI system for personal use without prior approval of the appropriate department leader.

VI. High-Risk Use of AI Systems.

There are certain uses of AI systems that are more high risk than others. As a global company, YourCompanyName is committed to complying with all AI legal requirements and guidance in the countries in which it operates. The European Union ("EU") has classified the following potential uses of AI as posing a high risk to the health and safety or fundamental rights of natural persons. Therefore, there are several additional requirements for the use of AI systems in such cases. These requirements are listed in Appendix II, with certain functions highlighted below:

- **Personal Data in AI Systems:** AI should be used with extreme caution when inputting any personal data of an individual into a closed AI system (it is prohibited to put any personal data into an open AI system).

- Screening Job Candidates: AI should be used with caution when screening any job applicants to ensure it does not adversely impact protected class members or introduce any bias. Equity and inclusion issues surrounding AI use in job screening are a potential source of litigation.

- **Personnel Decisions:** AI should be used with caution for any use related to making decisions on promotions, retention, or similar personnel such decisions. Extreme caution should be utilized to ensure that biases (including biases found in existing data sets) are avoided.

- **Enrollment Decisions:** Extreme caution should be utilized if using AI in any manner related to evaluating potential candidates for admission into a university, academy, internship or apprenticeship program, or any other YourCompanyName program.

- **Assessment of Students:** Any assessment of students in educational or vocational training institutions is considered high risk. Accordingly, extreme caution should be utilized before using any AI system intended to assess or evaluate any student participating in a course, taking an exam, or other evaluation or assessment.

VII. General AI System Use Standards and Use Approval

Except for AI Embedded Tools in approved software, all uses of AI systems must be approved by the AI Committee prior to use to ensure such AI system use meets the following principles:

- **Lawful:** The use of AI systems must comply with all applicable laws and regulations, as well as any contractual obligations, limitations, or restrictions.

- **Ethical:** The use of AI systems must adhere to ethical principles, be fair, and avoid bias.

- **Transparent:** There must be clear objectives for the use of an AI system and documented oversight of such use, which is recorded and captured for institutional knowledge. Disclosures of the use of AI in any AI-assisted content generation must be made when required by law or contract, or when required by the YourCompanyName.

- **Necessary:** The use of AI systems must be for a valid business purpose to improve YourCompanyName's business efficiencies and support the organization's mission. The use of AI is not a substitute for human critical thinking or expertise and should not require YourCompanyName to incur an unnecessary expense without any true benefit.

Prior to submitting a request to the AI Committee for the use of an AI system, a requester should first obtain the approval of his or her manager. In addition, in evaluating whether to make a request, the requester should ensure that the AI system use, if approved, would conform with the guidelines in this Policy, prior to submitting such request. Requests for the use of an AI system should follow the SOP here [INSERT LINK].

VIII. Training

All YourCompanyName Representatives who interact with AI systems must be trained on this Policy. Additionally, specific departments or functions at YourCompanyName may require more specific training on the use of AI systems for their department or function when more high-risk.

IX. Reporting Non-Compliance.

YourCompanyName directors, managers, employees, and agents aware of any conduct that may violate this Policy have a responsibility to report it. Individuals are encouraged to make reports through normal reporting relationships beginning with their manager. All reports of suspected misconduct or non-compliance will be investigated by the AI Committee, Legal Counsel, Human Resources, or other appropriate parties. Unless acting in bad faith, YourCompanyName employees will not be subject to reprisals for reporting potential violations.

If YourCompanyName determines that a YourCompanyName Representative has failed to comply with this Policy after an investigation concludes, then the YourCompanyName Representative will be subject to disciplinary action, up to and including termination.

ANNEX I
AI TECHNIQUES AND APPROACHES

- Machine learning approaches, including supervised, unsupervised, and reinforcement learning, using a wide variety of methods, including deep learning.

- Logic and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference, deductive engines, (symbolic) reasoning, and expert systems.

- Statistical approaches, Bayesian estimation, search, and optimization methods.

ANNEX II
EU High-Risk System Requirements

Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency, the provision of information to users, human oversight, robustness, accuracy, and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety, and fundamental rights, as applicable in the light of the intended purpose of the system, and no other less trade-restrictive measures are available, thus avoiding unjustified restrictions to trade.

High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely, and it does not become the source of discrimination prohibited by Union law. High-quality training, validation, and testing data sets require the implementation of appropriate data governance and management practices. Training, validation, and testing data sets should be relevant, representative, free of errors, and complete in view of the system's intended purpose. They should also have the appropriate statistical properties, including as regards the persons or groups of persons on which the high-risk AI system is intended to be used. Training, validation, and testing data sets should consider, to the extent required in the light of their intended purpose, the features, characteristics, or elements that are particular to the specific geographical, behavioral, or functional setting or context within which the AI system is intended to be used. To protect the rights of others from the discrimination that might result from the bias in AI systems, the providers should be able to process also special categories of personal data, as a matter of substantial public interest, to ensure the bias monitoring, detection, and correction in relation to high-risk AI systems.

For the development of high-risk AI systems, certain actors, such as providers, notified bodies, and other relevant entities, such as digital innovation hubs, testing experimentation facilities, and researchers, should be able to access and use high-quality datasets within their respective fields of activities which are related to this Regulation. European common data spaces established by the Commission and the facilitation of data sharing between businesses and with the government in the public interest will be instrumental in providing trustful, accountable, and non-discriminatory access to high-

quality data for the training, validation, and testing of AI systems. For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of artificial intelligence algorithms on those datasets, in a privacy-preserving, secure, timely, transparent, and trustworthy manner, and with appropriate institutional governance. Relevant competent authorities, including sectoral ones, providing, or supporting the access to data may also support the provision of high-quality data for the training, validation and testing of AI systems.

Having information on how high-risk AI systems have been developed and how they perform throughout their lifecycle is essential to verify compliance with the requirements under this Regulation. This requires keeping records and technical documentation, containing information necessary to assess the AI system's compliance with the relevant requirements. Such information should include the typical characteristics, capabilities and limitations of the system, algorithms, data, training, testing, and validation processes used, as well as documentation on the relevant risk management system. The technical documentation should be kept up to date.

To address the opacity that may make certain AI systems incomprehensible or too complex for natural persons, a certain degree of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should, therefore, be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to risks to fundamental rights and discrimination, where appropriate.

High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this purpose, appropriate human oversight measures should be identified by the provider of the system before it is placed on the market or put into service. Where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training, and authority to carry out that role.

High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness, and cybersecurity in accordance with

the acknowledged state of the art. The level of accuracy and accuracy metrics should be communicated to the users.

Technical robustness is a key requirement for high-risk AI systems. They should be resilient against risks connected to the limitations of the system (e.g., errors, faults, inconsistencies, unexpected situations) as well as against malicious actions that may compromise the security of the AI system and result in harmful or otherwise undesirable behavior. Failure to protect against these risks could lead to safety impacts or negatively affect fundamental rights, for example, due to erroneous decisions or wrong or biased outputs generated by the AI system.

Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behavior, and performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can leverage AI-specific assets, such as training data sets (e.g., data poisoning) or trained models (e.g., adversarial attacks), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures should therefore be taken by the providers of high-risk AI systems, also considering as appropriate the underlying ICT infrastructure.

Source: EU Artificial Intelligence Act, para. 43-51

ANNEX III
Potentially Applicable EU High-Risk System Types

- 'Real-time' and 'post' remote biometric identification systems. Both types should be subject to specific requirements on logging capabilities and human oversight.

- AI systems used in education or vocational training, notably for determining access or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education.

- AI systems used in employment, workers management, and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination, and for task allocation, monitoring, or evaluation of persons in work-related contractual relationships.

- Access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living. AI systems are used to evaluate the credit score or creditworthiness of natural persons.

Source: EU Artificial Intelligence Act, para. 33-37