Generative AI Policy of “ABC”

Purpose

ABC Entity ("ABC") recognizes the potential benefits and risks associated with the use of Generative AI (hereafter referred to as “Gen AI”). This Policy provides guidelines for the use of Gen AI by ABC and is intended to promote responsible and ethical use of this technology.

This Policy outlines ABC's commitment to the responsible implementation of this technology to ensure that its use aligns with our values, mission, business standards and security standards. It is critical that the associated risks of Gen AI are identified, mitigated as necessary, and appropriately managed on an ongoing basis in a rapidly-changing technical, business and regulatory environment. ABC is committed to balancing Gen AI risk with time to value.

Background

Gen AI, including technologies like ChatGPT developed by OpenAI and others, in addition to hosted domain models offered by other vendors, provides numerous textual, visual and auditory benefits, as well as others efficiency and marketing advantages, which ABC seeks to leverage where appropriate.

However, these technologies also pose a myriad of potential cybersecurity, ethical and legal risks, such as potential intellectual property law exposure, privacy law violations, and third-party actor risk including data breach. Gen AI also carries the potential for flawed, biased and/or inaccurate results. The Gen

AI landscape is evolving at an exponential rate, demanding tht all of us keep up with its pace of development. In this way, ABC can apply it appropriately and scale its use with confidence, while remaining in legal and ethical compliance.

This Policy provides guidance on practices that employees, consultants and other stakeholders acting on behalf of ABC, are required to adhere to in the use of Gen AI. The choice of AI providers in the pursuit of ABC's affairs will be limited to those determined by the Risk and Compliance Cybersecurity Team of ABC.

Risk Potential

Bias

AI systems learn from the data they are trained on, and thus can unintentionally perpetuate biases found in their training data set. Many large language models (LLMs) have filters to reduce the risk of bias or harmful outputs, but filters alone are insufficient. It is our ABC's responsibility to ensure that content we produce directly or by request, whether used internally or externally, is reviewed for potential bias to avoid any potential for discrimination.

Data Privacy Violations

The use of Gen AI can result in the breach of confidentiality and specific data privacy violations. We must protect the privacy of our customers, employees and other stakeholders by ensuring that our use of Gen AI complies with all relevant data privacy laws and regulations. This includes the GDPR of the EU, the California CCPA, privacy rules and regulations of other States, and other applicable regional or sector-specific regulations.

Security/Breach

AI provider systems can be targets for cyber-attacks. Security protocols are determined by our Risk and Compliance Cybersecurity Team and must be adhered to.

Ethical Considerations

Gen AI should not be used to mislead or manipulate customers. All content created using Gen AI should be ethical and, as such, in line with our mission statement and corporate values. Gen AI must be used ethically at the prompt request stage and all output content must be subject to thorough review for the elimination of ethical abuse.

Impersonation

All those operating on behalf ABC should not use Gen AI to impersonate any person without their express permission. Gen AI allows the facility, among many other uses, to create content “in the style” of public figures. ABC does not support this practice without prior authorization. Designated employees may, with permission and review, use Gen AI to mimic the writing style of a current ABC employee for the purposes of ghostwriting or editing content from that individual.

Data Poisoning

Data poisoning occurs when a bad actor "poisons" data by contaminating it with false data either by injection of new false data or tampering with existing data. Algorithmically, this may then produce false results. Further, bad actors may seek to create a route to hijack a Gen AI system.
Due to the extensive amount of data in use, this practice can be extremely difficult to detect. While the average designated user is not expected to

identify such issues, it points to the importance of using only the designated Gen AI providers specified by the Risk Management Cybersecurity Team.

Data Hallucinations

No system is entirely error-free. On occasion, a Gen AI provider may produce output that is randomly incorrect and/or not substantiated by the training data. Once again, while the average user is not expected to be familiar with the training data from which such hallucinations are derived, it highlights the importance of human review of generated output.

Intellectual Property Violations

In addition, ABC must also protect the privacy of our own intellectual property and that of our counterparties and customers. Once again, adherence to the approved list of Gen AI tools will help safeguard such and ensure that our data and IP, or other data to which we have access, is not used to train publicly accessible language models and other forms of Gen AI.

Risk Management

Operationally, ABC must first focus on identifying designated users and roles within ABC of Gen AI, by function if necessary. ABC will identify key oversight responsibility for Gen AI within our organization, will consult with third-party professionals as necessary, and will regularly review, identify and mitigate associated technical and legal risks for our organization. ABC will determine the suitable technology choices, including Gen AI Providers and risk management solutions, monitor business operations, and will implement a control system to manage and contain these risks on an ongoing basis.

At any given point, certain risks may have been identified. There will remain the potential for other as yet unknown risks as a function of the innate nature of Gen AI, its use internally and by third parties, and the changing legal and

regulatory framework around the world. Control procedures will be monitored by the Risk Management Cybersecurity Team to reflect these concerns.

Transparency

It is important that we at ABC remain as transparent as possible about our use of Gen AI. This includes acknowledging when AI is being used to create or modify content. This transparency can be effected through a blanket statement on our website and integrated into contracts with appropriate clients.

Example of a Transparency Statement:

The following is an example of a transparency statement on your use of Gen AI. Please edit it, along with this Policy as a whole to make it your own:

"At ABC, we use(d) Generative AI to assist in the development of some of our/this published content. To ensure quality control, transparency, accountability, and privacy standards, we adhere to the terms of our Generative AI Policy, including the use of internal technology solutions to manage any ongoing risk. Our Policy and tools help us to safeguard against biases or errors, maintain data security, and uphold our commitment to ethical marketing practices."

Review Function & Accountability

Responsibility should not be outsourced to a machine. We at ABC are ultimately legally responsible and morally accountable for our use of Gen AI. It is simply an assistant. It is not a replacement for good judgment. Our company Policy is that we should NEVER publish or send something that has been written entirely by Gen AI without human development and/or review for quality and accuracy. In circumstances of any negative outcomes from Gen

AI-assisted content, we at ABC must take full responsibility and take action as necessary.

Authorized Generative AI Tools

Please refer to ABC's list of Authorized Gen AI Providers below:

A
B
C

These Gen AI Providers have been subject to review by ABC's (appointed Artificial Intelligence Information Officer and) Risk Management Cybersecurity Team and have been judged to have met best-in-class security and privacy policies including SOC2 compliance, SSO and U.S. data storage. Absent separate authorization, no other Gen AI providers are to be used when acting on behalf of ABC or otherwise on ABC licensed software or ABC hardware for any purpose. Under no circumstances should any user submit ABC customer or other ABC counterparty data into Gen AI tools, including Large Language Models.

Appropriate Use Cases

ABC has identified the appropriateness of the use of Gen AI in the following departments/functions:

A
B
C

Inappropriate Use Cases

While there are many positive use cases of Gen AI assistance in our work, there are specific functions in respect of which we have decided as an organization to restrict the use of Gen AI. Do not use Gen AI for the following:

[Insert any uses that your company would like to restrict based on your own standards. Limited/no use use cases could include performance evals., legal contracts, specific coding projects, etc.]

Training and Awareness

All employees involved in creating content for ABC with Gen AI should receive appropriate technical and Policy awareness training. This should cover both the procedural aspects of using Gen AI, and the ethical considerations outlined in this Policy.

Acceptable Use

Employees and any others working on behalf of ABC should adhere to the following guidelines when using Gen AI:

- **Do not disclose confidential or proprietary information to a GenAI technology, directly or through a third-party application, unless following the guidelines of this Policy.**
- **Aways use Gen AI in a respectful and professional manner, refraining from using profanity, discriminatory language, or any other form of communication that could be perceived as offensive.**
- **Comply with all relevant laws and regulations, including those related to data privacy and information and security, all Policy procedures, training directives, and any incident response measures required, in accordance with this Policy.**

- **Report any concerns or incidents related to the use of Gen AI to their supervisor or the appropriate department, if not already clearly flagged by ABC's control solutions.**
- **Ensure that information being generated from Gen AI is reviewed by the designated supervisor, as appropriate, before being used for official work.**
- **Seek to understand the Gen AI system being used, to the extent of your knowledge, position and ability, including how it works and its potential limitations.**
- **Ensure that every new hire and existing employee responsible for Gen AI use has read this Policy and is adequately trained.**
- **For specific tools, document their functionality, limitations, and ABC's standards for using such technologies.**

Risk Management Cybersecurity Team

NOTE: The Risk Management Cybersecurity Team identified for ABC should consult also the "Gen AI Policy Template - Cybersecurity Addendum", to be read in conjunction with this Policy.

Please note that this Policy and the "Cybersecurity Addendum" are templates only and will need to be tailored to fit the specific needs and circumstances of your organization. Always consult with a legal professional when drafting policies to ensure compliance with all relevant laws and regulations. Always consult with a security professional when developing security checklists to ensure they adequately address all potential risks.

Gen AI Policy Template - Cybersecurity Addendum

Gen AI Implementation and Integration Guidelines

1. **Where possible, locally hosted versions of Gen AI should be used, particularly with respect to the efficient mining of internal data. Separation of Gen AI models may be necessary or advisable for different use cases. In all use cases, for both hosted versions and cloud-based Gen AI platforms, ensure sign-off of all Gen AI output by the designated Risk and Compliance team.**
2. **Use Gen AI technology responsibly, ensuring compliance with applicable laws and regulations, conducting regulatory review, risk assessments, and considering the potential impact on stakeholders. Prepare awareness campaigns for employees.**
3. **Identify any technology, infrastructure, or business processes reliant on Gen AI, implement appropriate safeguards or controls, log and archive all Gen AI usage according to applicable laws and regulatory requirements.**
4. **Identify all data, intellectual property, integrations, internal and external applications, and services that a Gen AI application might have access to. Implement proper security and access controls, providing the minimal access necessary for the Gen AI application to perform its tasks.**
5. **When building Gen AI integrations, evaluate and curate the appropriate providers by functionality and quality control. In conjunction with necessary advisors and legal resources, consider the regulatory context and requirements for audits and compliance; identify any risks to intellectual property; validate output for accuracy free from inaccurate or fabricated answers, biases or hallucinations, and; review protocols for data breach potential.**
6. **Ensure that the Legal and Compliance team reviews Gen AI output for any potential legal violations in a review schedule to be determined. Violations of Gen AI usage policies may result in disciplinary action, up to and including termination of employment.**

Generative AI Security Checklist

7. **Risk Assessment: Conduct a comprehensive risk assessment for the use of Gen AI technologies, considering potential threats, vulnerabilities, and impacts.**
8. **Data Privacy: Ensure that the use of Gen AI complies with all relevant data privacy laws and regulations. This includes the GDPR of the EU, the California CCPA, or any other applicable regional or sector-specific regulations.**
9. **Data Access Control: Implement strict access controls to ensure that Gen AI technologies can only access the data they need to function and nothing more.**
10. **Third-Party Risk Management: If using third-party Gen AI technologies, conduct a thorough review of the provider's security practices and ensure they meet your organization's standards.**
11. **Security Measures: Implement appropriate security measures to protect against unauthorized access to Gen AI technologies. This could include encryption, secure coding practices, and regular security testing.**
12. **Monitoring and Logging: Establish a system for monitoring and logging all interactions with Gen AI technologies. This can help detect any unusual or suspicious activity.**
13. **Data Anonymization: Ensure that all company and other sensitive data is removed from any prompt requests and confirmed in the human review of Gen AI output both for internal and external use.**
14. **Incident Response Plan: Develop an incident response plan that specifically addresses potential security incidents involving Gen AI technologies.**
15. **Employee Training: Provide regular training to employees on the secure use of Gen AI technologies, including familiarity with the Gen AI Policy of ABC. This should include guidance on what information can and cannot be shared with Gen AI technologies, human monitoring and data anonymization.**

16. **Regular Audits: Conduct regular audits of your Gen AI technologies and their use to ensure compliance with the Policy and to identify any potential security issues.**
17. **Review and Update: Regularly review and update your Gen AI Policy and security checklist to ensure they remain relevant as technology and associated threats evolve.**

Please note that this "Cybersecurity Addendum" and the related Gen AI Policy are templates only and will need to be tailored to fit the specific needs and circumstances of your organization. Always consult with a legal professional when drafting policies to ensure compliance with all relevant laws and regulations. Always consult with a security professional when developing security checklists to ensure they adequately address all potential risks.

—----------