THRIVE℠

AI Policy Template

Acceptable Use of Generative AI Tools

[Company Name]
IT Compliance Program

Acceptable Use of Generative AI Tools

Version 1.0 / Effective 01/01/23

AUS.AI. Acceptable Use of Generative AI Tools

AUS.AI.1. Scope

This policy applies to the use of any third-party or publicly available GenAI tools, including (but not limited to) ChatGPT, Google Bard, DALL-E, Midjourney, and other similar applications that mimic human intelligence to generate answers, work product, or perform certain tasks. This policy does not cover Generative AI or other AI tools that have been approved.

AUS.AI.2. Purpose

Publicly available applications driven by generative artificial intelligence (GenAI), such as chatbots (ChatGPT, Google's Bard, Microsoft Bing) or image generators (DALL-E 2, Midjourney) are impressive and widely popular. But while these content-generating tools may offer attractive opportunities to streamline work functions and increase our efficiency, they come with serious security, accuracy, and intellectual property risks. This policy highlights the unique issues raised by Generative AI, helps employees understand the guidelines for its acceptable use, and protects the Company's confidential or sensitive information, trade secrets, intellectual property, workplace culture, commitment to diversity, and brand. This Policy is intended to protect the interests of the company, its employees, and its stakeholders, and to provide guidance on acceptable and unacceptable uses of AI.

AUS.AI.3. Policy

Acceptable Use: AI shall be used in a professional, ethical, and lawful manner. Users shall respect the rights and privacy of others and shall not use the AI in any way that is illegal, harmful, or interferes with the use of the AI by others. AI programs shall not be used to produce or otherwise interact with information, images, files, or other digital content not related to company objectives, including obscene or potentially offensive content.

Privacy and Data Protection: AI shall not be used in a way that infringes upon individuals' privacy rights. The use of AI must comply with all applicable privacy laws and regulations and with our company's Data Protection Policy. Users are prohibited from inputting personally identifiable information or sensitive business information into third-party AI applications. Please reference the Data Classification Policy for details on restricted data.

Security: Users may be provided with access to [Company Name]'s owned AI platforms in accordance with their job responsibilities. As with all corporate technology systems and data, users must take all necessary precautions to prevent unauthorized access to the AI and to protect the integrity and security of the platform(s). This includes protecting passwords and other access information, updating and patching software as required, and reporting any suspected security breaches immediately to an executive.

Transparency: Where AI interacts with individuals, either internally or externally, it must do so in a transparent manner. Users must ensure that individuals are aware when they are interacting with AI and what data the AI is collecting, processing, or using.

Accuracy and Quality: Users must ensure that data used by AI is accurate, complete, and high-quality. Inaccurate or poor-quality data can lead to incorrect or biased decisions by the AI. Users are encouraged to also consider the context in which the output will be incorporated into business works for appropriateness and accuracy. All AI-produced works are subject to Q/A review process before incorporation into production data sets or product builds in compliance with the Software Development Policy standards.

Fairness and Non-Discrimination: AI must not be used in a way that discriminates against or harms individuals or groups based on characteristics such as race, color, religion, sex, national origin, age, disability, or genetic information.

Training and Supervision: Users must undergo appropriate training before using AI. The use of AI must be supervised by appropriately trained personnel who can understand and manage the risks associated with the use of AI.

Auditing and Monitoring: The use of AI will be subject to regular audits to ensure compliance with this Policy and with other applicable laws and regulations. The use of AI may also be monitored for compliance purposes.

Intellectual Property: Users must respect the intellectual property rights associated with AI. Unauthorized copying, distribution, or reverse engineering of AI is prohibited. Furthermore, employees are prohibited from using AI platforms to manipulate, alter, or otherwise reproduce copyrighted content for business purposes.

AUS.AI.4. Strategy

This policy supports the objective in Acceptable Use Strategy which states [Company Name] shall establish and promote acceptable uses of its Information Assets and related resources."

AUS.AI.5. Violations

Violations of this Policy may result in disciplinary action, up to and including termination of employment or contract, legal action, and/or reporting to relevant authorities.

AUS.AI.6. Terms & Definitions

Term	Definition
Classified information	Privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization or person who owns it.
Generative AI	A form of machine learning that is able to produce, text, video, images, and other types of content.
Security Incident Response	The act of reporting any suspected security breaches.
Intellectual Property	A work or invention that is the result of creativity, such as a manuscript or a design, to which one has rights and for which one may apply for a patent, copyright, trademark, etc.
Physical security	Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect Personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). It involves the use of multiple layers of interdependent systems which include closed circuit television (CCTV) surveillance, security guards, protective barriers, locks, access control protocols, and many other techniques.
Post-incident analysis	The process where the steps used to resolve a security incident and the issue that caused the incident are reviewed to learn how to better handle and if possible, prevent the incident from reoccurring.
Security breach	A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter.
Security incident	A security incident is a warning that there may be a threat to information or computer security. The warning could also be that a threat has already occurred.
Security violation	Internal act that bypasses or contravenes security policies, practices, or procedures. A similar external act is called security breach.