Presidio Trust

Compliance Plan for OMB Memorandum M-24-10

PRESIDIO
TRUST

September 20, 2024

PRESIDIO
TRUST®

REVISION HISTORY

Date	Name	Description of Change	Version
09/20/2024	IT Director	Initial Version	1.0

PURPOSE

The AI in Government Act of 2020 and OMB Memorandum M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence, direct each agency to submit to OMB and post publicly on its website either a plan to achieve consistency with M-24-10 or a written determination that the agency does not use and does not anticipate using covered AI.

This document outlines the minimum information required for Presidio Trust's compliance plans that will satisfy the requirements of Section 3(a)(iii) of M-24-10 and Section 104(c) of the AI in Government Act. The Presidio Trust will report compliance with the individual use-case-specific practices mandated in Section 5(c)(iv) and (v) of M-24-10 separately through the annual AI use case inventory.

STRENGTHENING AI GOVERNANCE

The Presidio Trust has no intention of developing any custom AI software. It will however procure software solutions from vendors that use AI in their products.

The Presidio Trust has updated its Staff Member Guidebook to include a section on the use of Generative Artificial Intelligence Usage on the Public Internet. This includes the use of products like Chat-GPT, Gemini, CoPilot, etc. The Presidio Trust will continue to assess this content and update as needed given the amount of change in the industry and attention given in media and from staff.

The Presidio Trust will also be updating its software procurement processes to comply with M-24-10 with special focus on the areas of most risk to our agency:

- Use of AI in Safety-impacting and Rights-impacting scenarios
- Use of Generative AI in all uses

AI Governance Bodies

Establishing AI Governance within the Presidio Trust is a critical component of our commitment to ensuring AI technologies' responsible and ethical use. The governance is designed to oversee the implementation and operation of AI systems and ensure compliance with relevant laws, regulations, and internal policies.

Composition of AI Governance Bodies

- The AI governance at the Presidio Trust will rely on representatives from various key departments, ensuring a comprehensive and multidisciplinary approach to AI oversight. The departments represented include Information Technology, Legal and Procurement.
- The Information Technology department, specifically the Director of IT, will have overall accountability and will report out to the Chief Operating Officer. At the Presidio Trust, the role of Chief AI Officer is a responsibility of the IT Director.

Expected Outcomes

AI governance at the Presidio Trust aims to achieve the following outcomes:

- **Ethical AI Deployment:** Ensure all AI systems are deployed consistently with ethical standards and organizational values.
- **Risk Mitigation:** Identify and mitigate potential risks associated with AI, including biases, unfair outcomes, and other harms.
- **Transparency and Accountability:** Maintain transparency in AI operations and hold stakeholders accountable for their roles in AI governance.
- **Continuous Improvement:** Foster a culture of constant improvement in AI governance practices, keeping pace with technological advancements and emerging best practices.

Consultation with External Experts

AI governance will include the consultation of external experts as appropriate and consistent with applicable laws. These consultations may include:

- **Industry Leaders:** Engaging with industry experts to gain insights into cutting-edge AI technologies and practices.
- **Interagency Collaboration:** Coordinating with other federal agencies to share knowledge and align on best practices for AI governance.

AI Use Case Inventories

The creation and maintenance of AI use case inventories are essential to ensuring that the Presidio Trust comprehensively understands how AI technologies are utilized across the agency. This inventory process allows us to manage AI deployments effectively, ensuring alignment with our ethical standards and regulatory requirements.

Process for Soliciting and Collecting AI Use Cases

The Presidio Trust will establish a systematic process for collecting AI use cases across all software systems.

This process includes:

- **Technology Review Intake Process:** Integrating AI use case collection into the existing technology review process to capture new AI initiatives at the proposal stage.
- **Continuous Monitoring:** Implementing ongoing monitoring mechanisms to identify emerging AI use cases and update the inventory accordingly.

Ensuring Comprehensive and Complete Inventory

To ensure that our AI use case inventory is comprehensive and complete, the Presidio Trust employs several strategies:

- **Stakeholder Engagement:** Engaging with key stakeholders, including IT Director, Technical Security Manager and other key stakeholders from IT to identify AI use cases.
- **Documentation and Tracking:** Maintain documentation in our internal systems inventory and track all AI use cases to ensure they are accurately represented in the Federal inventory.

Criteria for Excluding Use Cases from Federal Inventory

While the Presidio Trust aims to maintain a transparent inventory of AI use cases, certain use cases may be excluded based on specific criteria:

- Mission Risk: Use cases that, if disclosed, could negatively impact or create risks to the agency's mission, employees, customers, or the public.
- Confidentiality Agreements: Use cases subject to confidentiality agreements with other agencies, customers, employees, or stakeholders.
- Security Concerns: Use cases that involve sensitive or classified information that cannot be publicly disclosed.

Process for Periodic Review and Validation

The Presidio Trust is committed to periodically revisiting and validating the AI use cases in our inventory to ensure accuracy and relevance. This process includes:

- **Regular Reviews:** Conducting regular reviews of the AI use case inventory to identify any changes or updates needed.
- **Approval and Oversight:** The Chief AI Officer (CAIO), AI governance body, and senior leadership will be involved as needed in the review and validation process to ensure accountability and transparency.

ADVANCING RESPONSIBLE AI INNOVATION

At the Presidio Trust, we are committed to fostering an environment where AI technologies can be deployed and used responsibly. Leveraging AI's potential to enhance our operations and ensuring that such advancements align with ethical standards and regulatory requirements is one way of advancing responsible AI innovation.

The Presidio Trust has no intention of developing any custom AI software. It will however procure software solutions from vendors that use AI in their products. This will be done cautiously in areas that are low risk to start. The Presidio Trust will also take a test and learn approach using pilots to assess capability, risk and value.

Removing Barriers to the Responsible Use of AI

One of our primary goals is to identify and mitigate barriers to the responsible use of AI. We have undertaken several initiatives to achieve this:

- **Staff Guidance:** Published an update to our Staff Member Guidebook on the use of publicly available Generative AI tools (e.g. – ChatGPT). Held sessions with department leadership on pros and cons for the Presidio Trust and their department.

AI Talent

Given the size and scope of the Presidio Trust, we plan to only procure AI and to never develop it ourselves. Given this approach, our AI skills are narrowed down to the non-technical aspects of AI including how to best take advantage of it while taking on only appropriate risk.

AI Sharing and Collaboration

Given the size and scope of the Presidio Trust, we plan to only procure AI and to never develop it ourselves. Therefore, this section is not applicable in terms of sharing code, models, etc.

Harmonization of Artificial Intelligence Requirements

To ensure a consistent and unified approach to AI governance, innovation, and risk management, we plan to take steps to harmonize AI requirements across the agency:

- **Documentation of Best Practices:** Document and share best practices regarding AI usage, governance, innovation, and risk management to ensure they are consistently applied.
- **Continuous Improvement:** Update our AI practices and policies to reflect emerging trends, technological advancements, and evolving regulatory requirements.

MANAGING RISKS FROM THE USE OF ARTIFICIAL INTELLIGENCE

Determining Which Artificial Intelligence Is Presumed to Be Safety-Impacting or Rights-Impacting

To ensure the responsible deployment of AI, the Presidio Trust has established a process for determining which AI use cases are considered safety-impacting or rights-impacting:

- **Review Process:** Each new AI use case undergoes a review to assess whether it matches the definitions of safety-impacting or rights-impacting AI defined in Section 6 of OMB Memorandum M-24-10. This is done through our regular Technical Evaluation process which has been modified for this additional step.
  An additional review of existing software was performed for the software solutions that are used in safety-impacting and rights-impacting areas of the Presidio Trust.
- **Criteria for Assessment:** Our assessment criteria include the potential for physical harm, the impact on civil rights, and the degree of automation in decision-making processes.
- **Supplementary Criteria:** The Presidio Trust may develop additional criteria tailored to our specific operations to guide safety and rights-impacting AI decisions.

Implementation of Risk Management Practices and Termination of Non-Compliant AI

Implementing effective risk management practices is essential to mitigate the risks associated with AI:

- **Comprehensive Technical Evaluation Assessments:** Conduct comprehensive Technical Evaluations for all software. Evaluations include assessing the usage of AI, specifically in safety-impacting and rights-impacting usage.

Minimum Risk Management Practices

In certain circumstances, it may be necessary to issue waivers for one or more of the minimum risk management practices. The Presidio Trust has incorporated the approval process for this in the existing Technical Evaluation process that is performed for all software.

- **Waivers:** Granted only when necessary and justified.
- **Documentation and Transparency:** Maintain records of all waiver decisions to ensure transparency and accountability.

APPENDIX A: TERMS AND DEFINITIONS

Artificial Intelligence (AI) is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine and human-based inputs to perceive real and virtual environments, abstract such perceptions into models through analysis, and use model inference to formulate options for information or action.

Chief AI Officer (CAIO): A senior executive responsible for overseeing the agency's development and implementation of AI strategies, policies, and governance. The CAIO ensures compliance with ethical standards and regulatory requirements and coordinates AI initiatives across the organization.

AI Governance is the framework, processes, and policies implemented to ensure the ethical, legal, and responsible use of AI within an organization. It includes establishing governance bodies, principles, and guidelines to oversee AI applications.

Safety-Impacting AI: AI applications that have the potential to cause physical harm or pose significant safety risks. These use cases require rigorous risk assessments and compliance with stringent safety standards.

Rights-Impacting AI: AI applications that can potentially affect individuals' civil rights, privacy, or other fundamental rights. These use cases require careful consideration of ethical implications and compliance with legal and regulatory requirements.

Generative AI: A class of AI models that emulate the structure and characteristics of input data to generate derived synthetic content, such as images, videos, audio, text, and other digital content.

Risk Management Framework: A structured approach for identifying, assessing, mitigating, and monitoring risks associated with AI applications. The framework includes preventive controls, monitoring mechanisms, and procedures for managing incidents and non-compliance.

Incident Response Plan: A formalized set of procedures and protocols outlining the steps to respond to cybersecurity or operational incidents involving AI systems. The plan includes roles and responsibilities, communication protocols, and remediation actions.

Redress Mechanism: Processes and procedures established to address and resolve any harms or issues caused by AI systems. These mechanisms ensure that affected individuals or entities can report problems and seek remediation.

Bias Mitigation: Strategies and techniques aimed at identifying and addressing bias in AI applications to ensure fairness, equity, and inclusivity in decision-making processes and outcomes.

Transparency and Accountability: Principles ensuring that the development and deployment of AI systems are open and transparent, with clear documentation and oversight to hold stakeholders accountable for their roles in AI governance.

Ethical AI Use is the application of AI in a manner that aligns with ethical standards, respecting privacy, fairness, transparency, and accountability while avoiding harm to individuals and society.

Continuous Monitoring: Ongoing surveillance and assessment of AI systems to ensure they operate as intended and remain compliant with ethical standards, regulatory requirements, and performance expectations.

AI Talent Development: Initiatives and programs that aim to build and maintain a skilled AI workforce through targeted recruitment, training, and career development opportunities.

AI Ethical Use Policy: A set of guidelines and procedures that govern the use of AI within an organization, ensuring that AI applications align with ethical standards and organizational values.

Secure by Design is an approach to system design and development that integrates security considerations throughout the entire software development lifecycle, ensuring that AI applications are built with robust security measures from the outset.

Technology Review Process: A formal procedure for evaluating technology requests, including AI applications, to ensure they meet technical, ethical, and regulatory standards before approval and implementation.