

**COUNTY OF SAN DIEGO, CALIFORNIA
BOARD OF SUPERVISORS POLICY**

Subject	Policy Number	Page
	A-140	1 of 8

Purpose

This policy establishes a comprehensive, yet flexible, governance structure for Artificial Intelligence (AI) systems used by, or on behalf of, the County of San Diego (County). This policy enables the County to use AI systems for the benefit of the community while safeguarding against potential harms. The key objectives of this Policy are to:

- Provide guidance that is clear, easy to follow, and supports decision-making for the staff (full-time, part-time), interns, consultants, contractors, partners, and volunteers who may be purchasing, configuring, developing, operating, or maintaining the County’s AI systems or leveraging AI systems to provide services to the County.
- Ensure that when using AI systems, the County or those operating on its behalf, adhere to the Guiding Principles that represent values with regards to how AI systems are purchased, configured, developed, operated, or maintained.
- Define roles and responsibilities related to the County’s usage of AI systems.
- Establish and maintain processes to assess and manage risks and values presented by AI systems used by the County;
- Align the governance of AI systems with existing data governance, security, and privacy measures in accordance with the Administrative Manual section 0400-11 (County Info. Systems–Classification, Protection Level, & Proper Security)
- Define prohibited uses of AI systems;
- Establish “sunset” procedures to safely retire AI systems that no longer meet the needs of the County;
- Define how AI systems may be used for legitimate County purposes in accordance with applicable local, state, and federal laws, and existing County policies.

The County’s AI systems and the data contained therein will be purchased, configured, developed, operated, and maintained using the County’s AI Governance Framework.

Definitions

1. Artificial Intelligence: “Artificial intelligence” or “AI” to be a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, determinations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action. or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

**COUNTY OF SAN DIEGO, CALIFORNIA
BOARD OF SUPERVISORS POLICY**

Subject	Policy Number	Page
	A-140	2 of 8

Artificial Intelligence Board Policy

2. Algorithm: A series of logical steps through which an agent (typically a computer or software program) turns particular inputs into particular outputs.
3. AI system: Any system, software, sensor, or process that automatically generates outputs including, but not limited to, predictions, recommendations, or decisions that augment or replace human decision-making. This extends to software, hardware, algorithms, and data generated by these systems, used to automate large-scale processes or analyze large data sets.
4. Generative Artificial Intelligence (GenAI): GenAI is a subset of artificial intelligence that can create new, original content, such as text, images, videos, audio, and code, in response to a user's prompt. Unlike traditional AI, which is designed to analyze or classify existing data, GenAI produces novel outputs by learning patterns and structures from its training data.
5. Automated Decision Systems (ADS): A computational process, often powered by AI or machine learning, that makes or supports decisions, potentially impacting individuals, without requiring human intervention or judgment.
6. Human in the Loop (HITL): For purposes of this policy, a County worker in direct contact with an impacted constituent.
7. Surveillance: The systematic observation, monitoring, or collection of data regarding individuals, groups, or environments, often through the use of technology, to gather information for analysis or decision-making. This includes, but is not limited to, tracking behaviors, movements, or communications, and may involve the use of devices such as cameras, sensors, or software that analyzes data.

Scope

This policy applies to:

1. All AI systems deployed by the County or on the County's behalf; and
2. Staff (full-time, part-time), interns, consultants, contractors, partners, and volunteers who may be purchasing, configuring, developing, operating, or maintaining the County's AI systems or who may be leveraging AI systems to provide services to the County.

Guiding Principles for Responsible AI Systems

These principles describe the County's values with regards to how AI systems are purchased, configured, developed, operated, or maintained.

**COUNTY OF SAN DIEGO, CALIFORNIA
BOARD OF SUPERVISORS POLICY**

Subject	Policy Number	Page
Artificial Intelligence Board Policy	A-140	3 of 8

1. Human-Centered Design: AI systems are developed and deployed with a human-centered approach that develops, evaluates, and configures AI powered services for their impact on all stakeholders, including workers and the public.
2. Security & Safety: AI systems maintain confidentiality, integrity, and availability through safeguards that prevent unauthorized access and use. Implementation of AI systems is reliable and safe, and minimizes risks to individuals, society, and the environment.
3. Privacy: Privacy is preserved in all AI systems by safeguarding personally identifiable information (PII) and sensitive data from unauthorized access, disclosure, and manipulation. County employees must comply with all data privacy and security standards such as Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information (CJI), Criminal Justice Information Systems (CJIS), Internal Revenue Service (IRS), and the California Consumer Privacy Act (CCPA) to protect Personally Identifiable Information (PII), Protected Health Information (PHI), or any sensitive data used in AI.
4. Transparency: The purpose and use of AI systems is proactively communicated and disclosed to the public. An AI system, its data sources, operational model, and policies that govern its use are understandable and documented. Departments shall be responsible for determining the threshold above which text generated by an AI system is “substantial,” consistent with the principles outlined in this document as well as relevant intellectual property laws. All images and videos created by GenAI systems must be attributed to the appropriate GenAI system. Wherever possible, attributions and citations should be embedded in the image or video (e.g., via digital watermark).
5. Equity: AI systems support equitable outcomes for everyone. Bias in AI systems is effectively managed with the intention of reducing harm for anyone impacted by its use. County employees must leverage Justice, Equity, Diversity, and Inclusion (JEDI) team resources, especially uses that will analyze datasets or be used to inform decisions or policy.
6. Accountability:

Roles and responsibilities govern the deployment and maintenance of AI systems, and human in the loop (HITL) ensures adherence to relevant laws and regulations. CTO may revoke authorization for a technology that adds AI capabilities or may restrict the use of those AI capabilities, if, in its judgment, those AI capabilities present risks that cannot be effectively mitigated to comply with this policy or other County policies.
7. Effectiveness: AI systems are reliable, meet their objectives, and deliver precise and dependable outcomes for the utility and contexts in which they are deployed.
8. Workforce Empowerment: Staff are empowered to use AI in their roles through education, training, and collaborations that promote participation and opportunity.
9. Acquisition: The County’s standard for technology acquisition applies to all technology, including free-to-use software or software-as-a-service (SaaS) tools.
 - a. Consistent with the County’s standards for acquisition of technology resources, the County Technology Office (CTO) may authorize County employees to use pre-approved

**COUNTY OF SAN DIEGO, CALIFORNIA
BOARD OF SUPERVISORS POLICY**

Subject	Policy Number	Page
	A-140	4 of 8

GenAI software tools, or County employees may request an exception, or non-standard Notice of Decision (NOD) for acquisition or use of GenAI software through the CTO's current request process.

- b. If a technology that has already been approved for use in the County adds or incorporates different AI capabilities, County departments are required to initiate a re-evaluation by the CTO in accordance with enterprise architecture cloud review policy before the AI product features can be put into production. Also, all other aspects in this policy apply to said use.

Roles & Responsibilities

Several roles are responsible for enforcing this policy, outlined below:

- The Chief Information Officer (CIO), is responsible for directing County technology resources, policies, projects, services, and coordinating the same with other County departments. The CIO shall designate the Chief Technology Architect to actively ensure AI systems are used in accordance with the Administrative Manual section 0040-01 (County Information Systems – Management and Use).
- The Chief Technical Architect is responsible for ensuring that the County's use of AI systems is done so in accordance with this policy.
- The Chief Information Security Officer (CISO), or equivalent is responsible for overseeing the enterprise security infrastructure, cybersecurity operations, updating security policies, procedures, standards, guidelines, and monitoring policy compliance.
- The Chief Privacy Officer (CPO), or equivalent is responsible for overseeing the enterprise digital privacy practices, ethics, data processing practices, and responsible usage of technology in compliance with the Office of Ethics and Compliance.
- County departments are responsible for following this policy and following updates to this policy and the AI Governance Framework, and shall check compliance with these documents at least annually.
- The CIO or designee shall notify County departments when an update to this policy or the Governance Framework is released.
- The Office of County Counsel is responsible for advising of any legal issues or risks associated with AI systems usage by or on behalf of County departments.
- The County Technology Office may, at its discretion, inspect the usage of AI systems and require a department to alter or cease its usage of AI systems or a partner's usage of AI systems on behalf of the department.
- The Department of Purchasing and Contracting is responsible for overseeing the procurement of AI systems in alignment with existing IT procurement and governance processes and requiring vendors to comply with County policy standards through contractual agreements.

**COUNTY OF SAN DIEGO, CALIFORNIA
BOARD OF SUPERVISORS POLICY**

Subject	Policy Number	Page
	A-140	5 of 8

- The Office of Ethics Compliance & Labor Standards (OECLS) is responsible for enforcing labor standards and ensuring departments are following federal, state and local labor regulations.

Policy

When purchasing, configuring, developing, operating, or maintaining AI systems, the County will:

1. Uphold the Guiding Principles for Responsible AI Systems;
2. Conduct an AI Review to assess the potential risk of AI systems. The CIO or designee, is responsible for coordinating review of AI systems used by the County as detailed in the AI Governance Framework, specifically the Procurement Guidelines and Security Checklist;
3. Obtain technical documentation from vendors about specific AI systems being procured.. The Department of Purchasing and Contracting is responsible for requiring vendors to complete the AI Security Checklist;
4. Require contractors to comply with the CoSD AI Security Guidelines and CoSD AI Procurement Guidelines for AI Systems, or applicable legal addendum overseen by the Department of Purchasing and Contracting.
5. In the event of an incident involving the use of the AI system, the County will follow an Incident Response Plan as detailed in the AI Incident Response Plan. The CISO, or equivalent is responsible for overseeing the security practices of AI systems used by or on behalf of County departments;
6. Ensure outputs of GenAI systems are reviewed by a HITL prior to public consumption when used in an official County capacity. HITL review processes shall be documented by owning departments and shall describe how the HITL review was conducted to adhere to the principles outlined in this document. Furthermore, the right to override the outputs of the AI system shall be granted to the human in the loop, ensuring that human oversight is maintained. Where relevant, the department will establish criteria on when and how to override AI based decisions.
7. The owning department shall have County Compliance (or associated official compliance team) review the process.
8. Notify impacted constituents of the use of AI for the provision of particular County services and their right to alternatively access County such services (e.g. in person interview, paper application).
9. Inventory and publicly disclose the County's significant ADS use cases along with plain language explanations.
 - a. Significant ADS use cases are those that impact privacy, civil rights, or access to County services
10. Consult with diverse communities, stakeholders, workers and their representatives prior to deployment of any significant ADS to identify concerns, risks, and potential impacts of such ADS use cases.
11. Ensure that algorithmic impact assessments have been performed on significant ADS prior to

**COUNTY OF SAN DIEGO, CALIFORNIA
BOARD OF SUPERVISORS POLICY**

Subject	Policy Number	Page
	A-140	6 of 8

deployment and annually thereafter to identify systematic deviation.

12. Implement a procedure that allows individuals impacted by significant ADS to appeal negative outcomes to County staff empowered to resolve the situation.
13. Provide public notice at least 30 days prior to the adoption of new AI systems, to include specified use cases and an impact report. Where the new AI system includes surveillance technology, the public notice should also include a draft contract. Impacted worker groups should be consulted through meet-and-confer processes.
14. Produce an annual report on substantial AI, including any AI-assisted surveillance systems, with descriptions of changes in use cases, impacts, and documentation of all system feedback and complaints received over the previous year. Such annual report must be produced at least 30 days prior to the County's budget hearings.

Prohibited Uses

The use of certain AI systems is prohibited due to the sensitive nature of the information processed and severe potential risk. This includes the following prohibited purposes:

- Fully automated decisions that do not require any meaningful human-in-the-loop but substantially impact individuals.
- Covert use of AI systems to track individuals based on their behaviors, socioeconomic status, or personal characteristics, for any purpose, including social scoring.
- Cognitive behavioral manipulation of people or specific vulnerable groups.
- Employees are not permitted to use free-to-use GenAI websites or models that require the employee to create an account and agree to the terms and conditions of the GenAI company.

If County staff become aware of an instance where an AI system has caused harm, staff must report the instance to their supervisor and the Chief Privacy Officer.

AI System Sunset Procedures

If an AI system operated by the County or on its behalf ceases to provide a positive utility to the County's residents as determined by the Chief Information Officer, then the use of that AI system must be halted unless express exception is provided by the Chief Information Officer. If the abrupt cessation of the use of that AI system would significantly disrupt the delivery of County services, usage of the AI system shall be gradually phased out over time.

Public Records

**COUNTY OF SAN DIEGO, CALIFORNIA
BOARD OF SUPERVISORS POLICY**

Subject	Policy Number	Page
	A-140	7 of 8

The County is subject to the Board Policy A-54 (Public Access to County Records). County staff must follow all current procedures for records retention and disclosure.

GenAI solutions and/or vendors approved for County use shall be required to support retrieval and export of all prompts and outputs as well as model training details (either via exposed functionality or through vendor contract assurances).

Violations of the AI Policy

Violations of any section of the AI Policy, including failure to comply with the County's AI Governance Framework, may be subject to:

- Reporting of the incident(s) to management.
- Possible revocation of access privileges.
- Possible disciplinary action in accordance with Civil Service Rules, up to and including termination.

Violations made by a third party while operating an AI system on behalf of the County may result in a breach of contract and/or pursuit of damages. Infractions that violate local, state, federal or international law may be remanded to the proper authorities.

Exceptions

Staff, as described in the scope of this policy, must adhere to all controls outlined in this policy document unless a specific documented exception is explicitly granted by the Chief Information Officer. Policy violations that have not been formally documented as an exception will be treated as a security incident in accordance with County policy. County staff or Departments may encounter emergency situations that necessitate the immediate use of AI tools or technologies. In these circumstances, each incident use case must obtain documented approval via the Chief Information Officer prior to use. In such situations, the Department must submit the use case to the Chief Information Officer for review within 30 days of the incident.

The purpose of this policy is to help prevent the exfiltration of County data to personal devices which would violate Administrative Manual section 0400-11 (County Information – Classification, Protection Level, and Proper security). This approach allows employees to choose amongst various platforms which meet applicable privacy and security standards established by the County to facilitate productivity.

**COUNTY OF SAN DIEGO, CALIFORNIA
BOARD OF SUPERVISORS POLICY**

Subject	Policy Number	Page
	A-140	8 of 8

CTO will review exception requests according to its current compliance and security standards. CTO shall either approve, deny, or defer a request according to its adherence to compliance and security standards and the general principles within this policy.

The County Technology Office Chief Information Security Officer will designate a department to perform regular assessments of AI platforms and to regularly monitor such platforms so that the County can restrict and remove access in the event of a security or privacy incident.

Responsible Departments

1. County Technology Office
(CTO)

Attachment

County of San Diego Artificial Intelligence Bill of Rights.

Sunset Date

This policy will be reviewed for continuance by 12-31-2026.

Cross References

Board Policy A-54 (Public Access to County Records)

Board Policy A-111 (Data/Information and Information Systems)

Board Policy A-129 (Compliance with County-wide Records Management Program)

Board Policy A-131 (Privacy Protection)

Board Resolution 17-170 (Records Management)

Administrative Manual section 0010-17 (Equity and Racial Justice Administrative Policy)

Administrative Manual section 0040-09 (Document and Records Management Program)

Administrative Manual section 0040-10 (California Public Records Act procedures)

Administrative Manual section 0400-01 (County Info. Systems – Management and Use)

Administrative Manual section 0400-08 (County Info. Systems - Solutions Planning and Development of Requirements.)

Administrative Manual section 0400-11 (County Info. Systems– Classification, Protection Level, & Proper Security)

Administrative Manual section 0400-12 (Data and Performance Analytics)

DHR Policy and Procedures Manual section 01-115 (Code of Ethics)

DHR Policy and Procedures Manual section 01-117 (Social Networking)

NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0)