# Organizational AI Policy

## EXECUTIVE SUMMARY

### Problem and Purpose

AI can enter organizational work before leadership formally decides to “adopt AI” — through employees, contractors, suppliers, embedded software, enterprise services, and changing vendor capabilities. Without standing rules established before a disputed decision, failure, complaint, claim, or regulatory question occurs, the organization may be unable to demonstrate reasonable care, defined responsibility, appropriate verification, proper decision-making, required controls, and preserved evidence. The Policy exists to reduce that legal and financial vulnerability by establishing authoritative, operationally enforceable rules with only the minimum governance burden reasonably necessary for effective Control.

### Role in the AI Governance System

The AI Policy is the constitutional foundation of the OpExAI AI Governance System. It defines what must be true across organizational AI activity: purpose and authority, Modes of Operation, behavioral boundaries, risk logic, evidence expectations, competence, accountability, evolution, external alignment, and adoption/control. The RMS operationalizes the Policy during Normal Operations; the EMS or approved equivalent operationalizes it when Critical/Emergency governance is required.

### What the Policy Governs

- **Authorized and prohibited AI use —** who may use AI, what tools and information may be used.
- **Human responsibility and oversight —** AI does not assume organizational authority or responsibility; consequential use remains subject to responsible human judgment and applicable approval requirements.
- **Risk and evidence —** risk is classified by credible Consequence paths, and Medium/High-Risk activity preserves the decision-chain evidence needed for defensibility.
- **Suppliers, change, and system integrity —** supplier use, autonomous processes, significant change, continuity, and retirement remain governed as conditions evolve.
- **Modes of Operation —** the Policy defines Normal Operations and Critical/Emergency Operations and establishes when organizational behavior, authority, and response requirements must change.
- **Training, accountability, enforcement, and evolution —** the Policy remains operationally enforceable and current rather than becoming a static statement of principles.
- **Exceptions and controlled change —** legitimate temporary departures are handled through an authorized Policy Exception process, while permanent changes are made through controlled Policy amendment.
- **External release and autonomous operation —** externally released AI-assisted work and autonomous AI processes remain subject to defined risk, checking, authorization, and Control requirements.

© 2026 OpExAI.ai. All rights reserved.

- **Information and access control —** Restricted Information may be used with AI only in an authorized environment and for an authorized purpose, and AI-related activity must remain attributable to responsible Personnel or an authorized autonomous process

## Adoption and Operationalization

- **Customize before adoption —** the organization reviews and adapts the supplied Policy to its activities, governance, applicable legal/regulatory/contractual/insurance requirements, and risk environment.
- **Adopt and control the authoritative Policy —** formal approval establishes the governing version, ownership, scope, effective date, review cycle, and controlled copy.
- **Operationalize the rules —** adoption alone is insufficient. RMS, EMS, existing organizational processes, or approved equivalents must make the Policy real through roles, procedures, controls, training, evidence, monitoring, enforcement, and emergency readiness. The AI Deployment Consultant supports implementation when assistance is needed.

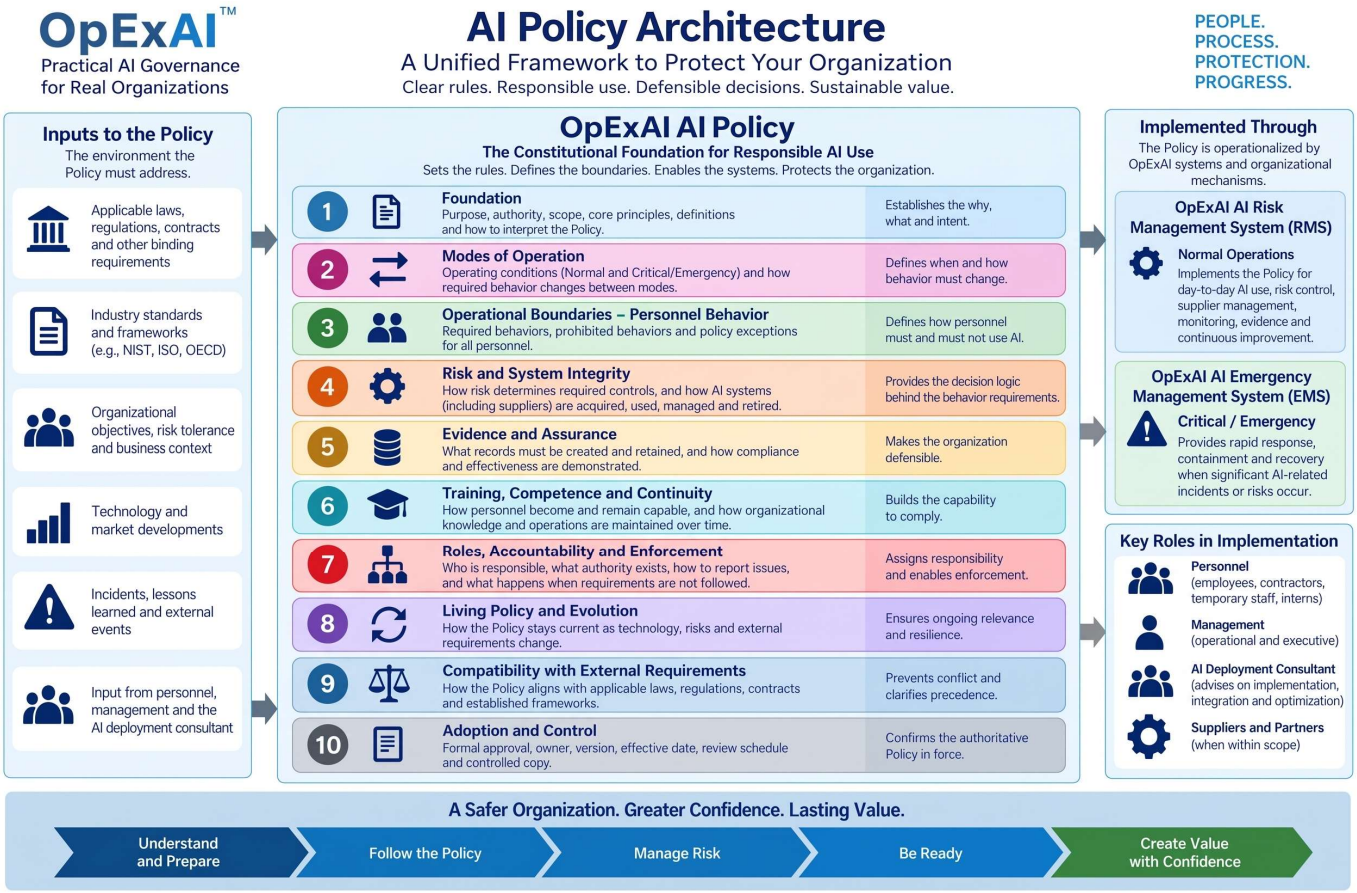
## Design Features and Benefits

- **Technology- and implementation-agnostic —** the Policy governs what technology does and how it is used rather than specific vendors, product names, workflows, or architectures.
- **Risk-proportionate and evidence-oriented —** governance focuses on consequential exposure and on evidence sufficient to demonstrate responsible decision-making and Control.
- **Operationally enforceable and living —** requirements are designed to govern actual behavior and remain current as technology, law, standards, suppliers, and organizational use change.
- **Framework-compatible —** the Policy is informed by major recognized governance, risk-management, cybersecurity, and emergency-management frameworks while preserving the precedence of applicable binding requirements.

© 2026 OpExAI.ai. All rights reserved.

# Policy Architecture

The Policy governs the full organizational AI lifecycle and defines the Modes of Operation that determine when organizational behavior and authority must change. Normal and emergency operating mechanisms implement different parts of the same constitutional foundation.




Applicable binding law, regulation, governmental order, contract, professional duty, insurance condition, and other controlling requirement remains controlling within its scope. The Policy is designed to operate with those requirements, not replace them.

© 2026 OpExAI.ai. All rights reserved.

# Framework Compatibility

The Policy is informed by recognized AI governance, risk-management, cybersecurity, and emergency-management frameworks. Compatibility is stated by function; it does not imply certification, clause-by-clause conformity, or that every technical or sector-specific control is contained in the Policy.

| Reference | Compatibility | Policy / System Interface |
|---|---|---|
| NIST AI Risk Management Framework + Generative AI Profile | Strong functional compatibility | Governance, accountability, risk identification, AI-result review, evidence, monitoring, improvement, change, and supplier controls align in function. Technical/sector testing depth remains use-specific and belongs in the applicable implementation. |
| ISO/IEC 42001:2023 | Strong management-system compatibility | Policy authority, risk management, roles, competence, documented information, monitoring, review, improvement, and lifecycle control align in function. No certification or clause-by-clause conformity claim is made. |
| ISO/IEC 23894:2023 | Strong risk-management compatibility | AI risk is integrated into organizational processes, contextualized, proportionate, and change-triggered. Internal OpExAI Risk Levels remain an implementation choice unless law or another binding requirement controls. |
| OECD AI Principles | Broad compatibility | Responsibility, rule-of-law precedence, transparency where required, robustness/security interfaces, accountability, and traceability are addressed. Jurisdiction- and sector-specific rights obligations remain subject to applicable requirements. |
| EU AI Act - Regulation (EU) 2024/1689 | Compatible as a governance base; not self-sufficient for EU compliance | EU legal roles, prohibited practices, literacy, transparency, high-risk classifications, and other duties control when applicable and cannot be replaced by OpExAI Low/Medium/High Risk Levels. An organization subject to the Act must map and implement those duties separately. |
| NIST SP 800-61 Rev. 3 / Cybersecurity Framework 2.0 | Interface compatible | Cybersecurity response remains within the organization's cybersecurity process. The external term "incident" retains its cybersecurity meaning in that domain. |
| FEMA NIMS / Incident Command System | Emergency-interface compatible | Defined command, modular organization, objectives, information management, resource coordination, and transfer of command are compatible at the architecture level. The EMS or equivalent emergency mechanism carries detailed emergency operations. |
| ISO 22320:2018 | Emergency-interface compatible | Roles/responsibilities, tasks/resources, coordination, and joint direction align at the emergency-management architecture level. Detailed operation remains in the EMS or equivalent mechanism. |

**Important:** Applicable binding law, regulation, governmental order, contract, professional duty, insurance condition, and other controlling requirements remain controlling within their scope. The Policy is designed to operate with those requirements, not replace them.

© 2026 OpExAI.ai. All rights reserved.