Monreal IT
Building Powerful Partnerships

AI GOVERNANCE STARTER KIT

AI Acceptable Use Policy Starter Kit

Copy-ready guardrails for safer, more productive AI use at work

Managed AI + Managed IT + Cybersecurity

monrealit.com | info@monrealit.com | 440.373.5805

Executive Introduction

Employees are already experimenting with artificial intelligence. Clear, practical guardrails reduce risk while helping teams use AI responsibly and productively. This starter kit provides a framework for establishing a foundational AI policy.

How to Use This Kit

1. **Assign ownership:** Designate a policy owner responsible for customization, implementation, and review.
2. **Complete the bracketed fields:** Replace each field with organization-specific information.
3. **Align with legal and compliance requirements:** Have qualified legal counsel and HR review the policy for relevant industry, state, and federal obligations.
4. **Train staff:** Ensure employees understand the policy and its implications.
5. **Review annually:** Update the policy as technology, regulations, and business needs evolve.

Important: This starter template is educational and does not constitute legal advice. Obtain qualified legal and HR review before adoption.

One-Page Launch Checklist

☐ **Executive Sponsor Identified:** A senior leader champions the policy.

☐ **Policy Owner Assigned:** One person is accountable for policy management.

☐ **Approved Tools Inventory Created:** Sanctioned AI tools and platforms are documented.

☐ **Data Classification Rules Defined:** Guidelines address different sensitivity levels.

☐ **Security Review Completed:** IT/Security has assessed risks and controls.

☐ **Legal and HR Review Conducted:** The policy aligns with legal and employment obligations.

☐ **Employee Training Scheduled:** A comprehensive education program is planned.

☐ **Acknowledgment Process Established:** The organization can capture employee agreement.

☐ **Incident Response Path Defined:** Reporting and response steps are documented.

☐ **Policy Review Date Set:** The next review is scheduled.

AI Acceptable Use Policy Template

[Organization Name] AI Acceptable Use Policy

Organization	[Organization Name]	Effective date	[Effective Date]
Policy owner	[Policy Owner]	Approved by	[Approver]
Review date/owner	[Review Date / Review Owner]	Version	[Version]

Purpose and Guiding Principles

This policy establishes guidelines for the responsible and secure use of artificial intelligence (AI) technologies within [Organization Name].

- **Business value:** Use AI to enhance productivity, innovation, and efficiency.
- **Protect confidential information:** Safeguard company, client, employee, and personal data.
- **Human accountability:** Humans remain accountable for decisions and actions assisted by AI.
- **Transparency:** Be clear about the use of AI in organizational work.
- **Fairness:** Prevent AI from perpetuating bias or producing unfair outcomes.
- **Security and compliance:** Maintain robust controls and comply with applicable laws, contracts, and policies.

Scope

This policy applies to:

- Employees (full-time and part-time)
- Contractors and temporary staff
- Interns
- Vendors and third parties accessing organizational systems or data

It covers publicly available AI tools, enterprise AI solutions, embedded AI features, private assistants and agents, and AI-powered automated workflows.

Approved Tools and Accounts

- **Approved tools only:** Use tools sanctioned by [Organization Name]'s IT and Security teams.
- **Business-managed accounts:** Use organization-provided or managed accounts for business work.
- **No personal or unapproved accounts:** Do not use personal accounts or unapproved tools for organizational work.
- **New-tool approval:** Submit requests to [Approved-Tools Contact] for security, privacy, and business-necessity review before implementation.

Approved AI Tools Register

Tool name	Approved purpose	Business data allowed	Owner	Review date

Data Handling Rules

Handle data according to its classification. Use approved enterprise AI tools for Yellow and Red data, subject to the controls below.

Classification	Rule	Examples
Green: Public	May be used in approved tools when the information is intended for public release or presents minimal disclosure risk.	Public news, press releases, public marketing materials, general industry knowledge
Yellow: Internal / Sensitive	Use only approved enterprise tools with appropriate security controls. Disclosure could cause moderate harm to [Organization Name], its clients, or employees.	Internal project plans, non-public research, draft marketing, internal metrics, basic employee contact details
Red: Restricted	Never enter into public AI tools. Use requires explicit authorization, documented controls, and an approved secure enterprise environment.	Client confidential data, regulated records, privileged material, non-public financials, trade secrets, sensitive personal data

Acceptable Uses

AI may assist with the following tasks when the approved-tool, data-handling, and human-review requirements are satisfied:

- **Brainstorming:** Generate ideas and explore concepts.
- **Drafting:** Create initial versions of documents, email, or presentations.
- **Summarization:** Condense approved content for quicker understanding.
- **Research:** Gather information from public or approved internal sources, with human verification.
- **Meeting notes:** Transcribe and summarize meetings with participant consent.
- **Analysis:** Analyze approved datasets using sanctioned tools.
- **Translation:** Translate approved content.
- **Code assistance:** Draft, debug, and optimize code in approved secure environments.
- **Knowledge retrieval:** Use approved internal knowledge sources.
- **Workflow automation:** Automate routine tasks within defined, approved boundaries.

Prohibited Uses

- Using unapproved AI tools or platforms for organizational work.
- Entering Restricted (Red) data into any AI tool without explicit authorization and documented controls.
- Creating or distributing deepfakes, impersonations, deceptive content, malware, or material that bypasses security controls.
- Making discriminatory, unlawful, biased, or unsupervised high-impact decisions.
- Publishing AI-generated output without human review and verification.
- Recording conversations or generating personal content without required consent.
- Bypassing licensing terms, intellectual-property rights, or usage restrictions.
- Generating content that violates [Organization Name]'s code of conduct or other policies.

Human Review Requirements

All AI-generated output used for business purposes requires careful human review. The reviewer must confirm:

- **Accuracy and sources:** The output is reliable and supported by credible sources.
- **Bias and fairness:** The output is free from unlawful or unfair bias.
- **Confidentiality:** No confidential or restricted information was exposed.
- **Tone and brand alignment:** The output matches [Organization Name]'s communication standards.
- **Intellectual property:** The output does not infringe copyrights, patents, or other rights.
- **Contractual commitments:** The output does not violate agreements or create unauthorized commitments.
- **Final approval:** A designated human approves the output before publication or action.

Accountability: AI may assist, but accountable humans own all decisions and communications.

Transparency and Disclosure

- **Internal disclosure:** Disclose material AI assistance to colleagues or managers when appropriate.
- **External disclosure:** Disclose AI assistance when required by law, policy, contract, or the nature of the work.
- **Synthetic media:** Clearly label AI-generated or significantly altered images, audio, and video.
- **No independent-verification claim:** Do not represent AI output as independently verified or guaranteed by [Organization Name] unless it has undergone appropriate human review.

Security Controls

- **Multi-factor authentication:** Enable MFA on all AI platform accounts.
- **Least privilege:** Grant only the minimum permissions required.
- **Approved integrations:** Connect AI tools only to approved internal systems.
- **Logging and retention:** Log and retain AI usage and outputs according to policy.
- **Vendor risk review:** Assess AI service providers regularly.
- **Secure configuration and patching:** Maintain supported, securely configured platforms.
- **No shared credentials:** Do not share AI platform login credentials.
- **Prompt-injection awareness:** Treat untrusted instructions as suspicious and report concerns.

Intellectual Property and Copyright

- **Upload rights:** Do not upload material unless the organization has the right to use it.
- **Usage rights:** Understand ownership and usage terms for AI-generated material.
- **Infringement review:** Review generated material for copyright or patent concerns.
- **Protect organizational IP:** Do not enter [Organization Name]'s proprietary information or trade secrets into public AI tools.
- **Attribution:** Provide attribution when required.

Automated Agents and Actions

- **Limited permissions:** Grant agents only the permissions required for their assigned tasks.
- **Human approval required:** Require approval before external communications, financial changes, record deletion, access changes, external publishing, or client commitments.
- **Testing:** Test agents in controlled environments before deployment.
- **Documentation and rollback:** Document capabilities, human overseers, logs, exception handling, and rollback procedures.

Incident and Concern Reporting

If you suspect or witness an AI-related incident:

1. **Stop use:** Immediately stop using the tool or feature in question.
2. **Preserve details:** Without spreading sensitive content, record the date, time, tool, prompt, output, and other relevant facts.
3. **Notify:** Report the incident through [Incident-Reporting Contact].

Examples include wrong-recipient output, sensitive-data exposure, harmful or unlawful content, unauthorized agent actions, and suspected account compromise.

No retaliation: [Organization Name] prohibits retaliation against anyone who reports a concern in good faith.

Training, Monitoring, Enforcement, Exceptions, and Review

Training: Employees will receive mandatory training on this policy and responsible AI use.

Monitoring: [Organization Name] may monitor AI use on organizational systems to verify compliance, subject to applicable law and policy.

Enforcement: Violations may result in disciplinary action, up to and including termination of employment or contract.

Exceptions: Exceptions must be requested and approved in writing by [Exception Approver].

Policy review: This policy will be reviewed at least annually by [Review Owner] and updated as needed.

Exception Request Form

Employee name	
Department	
AI tool/use case	
Reason for exception	
Proposed safeguards	
Requested by / date	
Approved by / date	

Employee Quick-Reference: Before You Use AI

Ask yourself these five questions:

1. **Is the tool approved?** Am I using a platform sanctioned by [Organization Name]?
2. **Is the data allowed?** Am I using the correct enterprise tool and keeping Restricted data out unless explicitly authorized?
3. **Can I verify the answer?** Is the output accurate, reliable, and fact-checked?
4. **Does a person need to approve it?** Is there a human review step for critical decisions or external communications?
5. **Would I be comfortable explaining this use?** Am I acting transparently, lawfully, and ethically?

Employee Acknowledgment

I have read, understood, and agree to comply with the AI Acceptable Use Policy. I understand that failure to follow this policy may result in disciplinary action.

Employee name (print)	
Employee signature	
Date	

Questions about this policy? Contact [Policy Contact].

30-Day Rollout Plan

Week 1 Discover & Inventory	Identify current AI use, finalize data classifications, and confirm the policy owner and executive sponsor.
Week 2 Approve & Customize	Approve initial tools, complete organization-specific policy fields, and obtain legal and HR review.
Week 3 Configure & Train	Implement technical controls, schedule employee training, and prepare communications.
Week 4 Launch & Measure	Launch the policy, collect acknowledgments, and establish monitoring and reporting.

Need help turning this starter kit into operational controls?

monrealit.com/ai-governance | info@monrealit.com | 440.373.5805

This starter kit is educational and does not constitute legal advice. Obtain qualified legal and HR review before adoption.