32 Kearney Road
Needham, MA 02494

Generative AI Policy & Usage Best Practices

A Practical Framework for Secure, Responsible, and Effective Enterprise Adoption

Executive Summary

Generative Artificial Intelligence (GenAI) is rapidly transforming how organizations create content, analyze information, and enhance productivity. However, without appropriate governance and safeguards, GenAI introduces risks related to data security, privacy, accuracy, and compliance.

This whitepaper outlines a practical, enterprise-ready framework for:

- Governing GenAI usage
- Protecting sensitive information
- Ensuring responsible and compliant adoption
- Maximizing business value while mitigating risk

The approach aligns with leading frameworks such as the NIST AI Risk Management Framework (AI RMF) and NIST Cybersecurity Framework (CSF), emphasizing governance, accountability, and human oversight.

1. The Role of GenAI in the Enterprise

GenAI tools (e.g., ChatGPT, Copilot, Gemini, Claude) enable users to generate text, code, and insights from natural language prompts. When used appropriately, they can:

- Improve productivity and efficiency
- Accelerate content creation
- Support research and analysis
- Enhance decision support

However, GenAI is not a decision-maker. It is a tool that must operate within defined controls and human oversight.

2. Core Principles for Responsible GenAI Use

Organizations should anchor GenAI adoption in the following principles:

A. Governance & Accountability

- Define clear ownership and oversight structures (e.g., AI Governance Committee)
- Require use of approved tools and enterprise-managed accounts only
- Ensure users are accountable for both inputs (prompts) and outputs

B. Human Oversight

- AI augments human judgment. It does not replace it.
- All outputs must be reviewed before use

C. Risk-Based Usage

- Align use cases with defined risk categories (permitted, restricted, prohibited)

D. Data Protection First

- Treat GenAI as a potential data exposure vector
- Apply strict data classification and handling controls

E. Transparency

- Disclose AI usage when it materially contributes to business outputs

3. Approved Tools & Controlled Environments

Organizations should explicitly define approved GenAI tools, typically including enterprise versions of:

- ChatGPT (OpenAI)
- Microsoft Copilot
- Google Gemini
- Anthropic Claude

Critical Requirement: Enterprise / Private Mode

GenAI tools must be used in private or enterprise configurations:

Mode	Risk Level	Key Characteristics
Public Mode	High Risk	Data may be retained, reused, or exposed outside organizational control
Private/Enterprise Mode	Lower Risk	Data not used for training, governed by enterprise agreements

If private mode cannot be verified, the tool should be treated as high risk, and sensitive data must not be used.

AI Policy: Start Restrictive, Expand Deliberately

Every organization's AI policy should begin from a position of restriction and expand only through a deliberate, documented approval process. This "restrictive-by-default" posture protects the organization while creating a structured path to adoption. The following example policy language illustrates this approach:

Sample Policy Language: Artificial Intelligence

AI tools are currently not approved for general use.

- An exception list will be maintained by IT and published on the company intranet.
- Access to AI tools and features may be requested via the Help Desk and, if approved, will be added to the exception list.
- Company data is considered Confidential Proprietary Business Information and must never be input into an AI system.
- Employees are expressly prohibited from using AI (generative or otherwise) to generate work product without explicit approval for that specific use case.

Organizations should adapt this baseline language to their specific risk tolerance and operational context. The key principle: define what is not permitted first, then create a clear, accessible process for exceptions and approvals.

4. AI Tool Evaluation and Approval Process

A structured, documented process for evaluating and approving AI tools is essential. This process must be visible and accessible to all employees, so they know how to request a tool and where to find the current approved list.

Process Requirements

- Provide a clear, easy-to-find mechanism for end users to request an AI tool evaluation (e.g., via Help Desk ticket or a designated intake form).
- Maintain a published, up-to-date list of approved AI tools on the company intranet, including approved use cases for each tool.
- Document the evaluation criteria and record the results of every evaluation—including the specific use cases assessed, the data types involved, and the final approval or denial decision.
- Assign ownership of the approved tools list to a named team or individual (typically IT, Security, or the AI Governance Committee) accountable for keeping it current.

5. AI Tool Evaluation Criteria

When evaluating any AI tool for potential approval, document the answers to the following questions:

- **What is the specific tool and use case?** Define the tool by name and version, and document the exact business use case being evaluated. Approvals are use-case specific.
- **What data will be used with the tool?** Classify the data (public, internal, confidential, regulated) and confirm it is appropriate for use with this tool under the approved configuration.
- **Where does the data sit?** Determine whether the tool is a shared public resource or a private instance within your organizational tenant. Confirm whether data is processed or transmitted outside your tenant for any reason, and whether any artifacts (e.g., transcripts, logs, chat history) are retained. Verify whether those artifacts can be aged off or deleted, and document the process for doing so.
- **What is the vendor's cybersecurity posture?** Research the vendor's track record, their published approach to cybersecurity, and any past incidents of concern. A

vendor with a poor or opaque security history should require heightened scrutiny or may warrant denial.

- **What is the contractual relationship?** Confirm whether the organization has a formal agreement in place, such as a contract, Non-Disclosure Agreement, Master Service Agreement, or Data Processing Agreement, or whether the tool is being accessed via a consumer or prosumer subscription with no organizational protections.

6. Periodic Reevaluation of Approved Tools

AI tools are not static. Vendors regularly release new versions, expanded capabilities, updated data-handling practices, and changes to underlying models, any of which may alter the risk profile of a previously approved tool. Approval is therefore not permanent.

Organizations must schedule and conduct periodic reevaluations of all approved AI tools. At minimum, reevaluation should be triggered by:

- A major version update or new feature release by the vendor
- Changes to the vendor's data handling, privacy policy, or terms of service
- A reported security incident or newly identified vulnerability associated with the tool or vendor
- Changes in applicable regulations or organizational data classification
- Annually, as part of the standard policy lifecycle review, regardless of vendor-side changes

The results of each reevaluation, including any changes to approval status or approved use cases must be documented and communicated to affected users promptly.

7. Permitted, Restricted, and Prohibited Use Cases

A clear use classification model is essential:

Permitted (Low Risk)

- Drafting emails, reports, and documents
- Summarizing non-sensitive information
- Brainstorming ideas

- Editing grammar and tone
- Creating templates and outlines
- Research using public data

Restricted (Moderate Risk – Requires Review)

- Legal or contractual content
- External communications
- HR or employee-related content
- Financial or executive materials
- Any use involving internal data

Prohibited (High Risk)

- Inputting sensitive or confidential data without approval
- Using personal accounts for business purposes
- Generating deceptive, harmful, or misleading content
- Making employment or high-stakes decisions
- Impersonation or fraud-related use

8. Data Protection & Privacy Requirements

Golden Rule

If you wouldn't send it externally, do not input it into GenAI.

Allowed Data

- Public information
- Generic or non-sensitive content
- Fully anonymized examples

Restricted / Prohibited Data

- Personally Identifiable Information (PII)

- Employee or HR data
- Financial data
- Contracts or legal documents
- Confidential or proprietary information

Best Practices

- Use minimum necessary data
- Anonymize whenever possible
- Avoid uploading files unless explicitly approved

9. Prompting Best Practices

Effective and secure prompting is critical.

Do

- Keep prompts general and non-sensitive
- Use anonymized or summarized inputs
- Limit context to what is strictly necessary

Don't

- Input internal documents or sensitive data
- Include identifiable company information unnecessarily

Example:

- ✅ "Summarize best practices for operational efficiency"
- ❌ "Summarize this internal company report"

10. Output Validation & Risk Management

GenAI outputs are inherently unreliable without validation.

Required Validation Steps

- Verify factual accuracy
- Check for hallucinations (fabricated content)
- Confirm sources independently
- Review for bias and appropriateness

Outputs should always be treated as draft content until validated.

11. Accuracy, Bias, and Ethical Considerations

GenAI systems can:

- Produce incorrect or outdated information
- Reflect bias or unintended assumptions
- Present false information confidently

Organizations must:

- Require critical review
- Involve subject matter experts where needed
- Implement bias-awareness practices

12. Security Controls & Safe Usage

To mitigate cybersecurity risks:

- Use only approved tools and managed accounts
- Disable unapproved plugins or integrations
- Avoid uploading sensitive files
- Be cautious of AI-generated phishing or malicious content
- Ensure alignment with broader cybersecurity policies

13. Monitoring, Reporting, and Incident Response

Organizations should establish clear reporting protocols.

Users must report:

- Accidental data exposure
- Misuse of GenAI tools
- Suspicious or unsafe outputs
- Security concerns

Prompt reporting enables rapid mitigation and aligns with incident response practices.

14. Transparency & Disclosure

Disclosure is required when GenAI significantly contributes to:

- External communications
- Client deliverables
- Policies or formal documents

Example Statement:

“This document was developed with the assistance of an approved AI tool and reviewed by qualified personnel.”

15. Training & Organizational Readiness

Effective GenAI adoption requires:

- Mandatory user training
- Ongoing awareness programs
- Clear, accessible policies and guidance
- Periodic policy updates

Training ensures users understand both capabilities and risks.

16. Governance Model

A mature GenAI program includes:

AI Governance Committee

Responsible for:

- Approving tools and use cases
- Overseeing risk management
- Ensuring regulatory alignment
- Maintaining policy lifecycle

Policy Lifecycle

- Annual review (minimum)
- Continuous updates based on technology and risk evolution
- Periodic reevaluation of all approved AI tools—triggered by version updates, capability changes, vendor policy changes, security incidents, or regulatory updates—with results documented and communicated to users

17. Quick Decision Framework for Users

Before using any AI tool, work through the following checklist. Every question should have a clear, confident "yes" before you proceed. If any answer is no or unclear, do not proceed.

- **Is the AI tool on the approved usage list?** Check the current approved tools list on the company intranet before using any AI tool. If it is not listed, submit a request through the Help Desk.
- **Is the intended use approved?** Approvals are use-case specific. Confirm that your specific intended use—not just the tool itself—has been evaluated and approved.
- **Is the data public or Confidential Proprietary Business Information?** Company data must never be input into an AI system unless that specific data type has been explicitly approved. When in doubt, treat data as confidential and do not proceed.

- **Am I using a company-managed account?** Never use personal accounts for business purposes. Personal accounts lack organizational protections and may expose company information.
- **Do you know where any artifacts of the tool reside?** Some tools retain transcripts, logs, or session history. Know where these artifacts are stored and whether they fall within your organizational control.
- **Do you know how to delete or age off any artifacts?** Before using a tool, confirm the process for removing session data, transcripts, or other residual artifacts, and follow that process consistently.
- **Are you using the tool to support a human process, or replacing one?** AI tools should augment human judgment, not replace it. If this use case removes a human decision point entirely, it requires explicit review and approval before proceeding.
- **Do you have a plan to review the results for accuracy and hallucinations?** AI outputs must always be treated as draft content. Define who will review the output, using what criteria, before it is used or shared.
- **Do you need to disclose the use of AI in this process?** Disclosure is required when AI materially contributes to external communications, client deliverables, or formal documents. If unsure, disclose.
- **Is training required for effective use?** Some approved tools require specific training before use. Confirm whether training has been completed and is current for this tool and use case.

If any answer is **no or unclear, do not proceed.**

18. Key Takeaways

- GenAI is a productivity tool, not a decision-maker
- Data protection is the top priority
- Always validate outputs before use
- Use only approved tools and environments
- Maintain human accountability at all times

Conclusion

GenAI presents significant opportunities for innovation and efficiency, but only when deployed responsibly. Organizations that implement strong governance, enforce data protection controls, and prioritize human oversight will be best positioned to unlock value while minimizing risk.