Prompt:

AI Acceptable Use Policy Checklist

Document Control

- □ Populate version history: Version #, Date, Author, Change Summary.
- □ Add policy owner, approver, and review schedule.
- □ Store the final policy in your policy repository and notify stakeholders.

Purpose & Scope

- □ Confirm that the policy clearly states the purpose: to promote safe, ethical, and compliant AI use.
- □ Validate that the scope includes all relevant users: employees, contractors, vendors, partners, etc.
- □ Ensure the scope includes both internal and third-party AI systems (including GenAI and agents).

Definitions

- □ Include key terms used in the policy (e.g., AI, GenAI, AI Agent, LLMs, Sensitive Data).
- □ Adapt definitions from reputable frameworks (Gartner, NIST, ISO) and clarify any internal jargon.

Acceptable Use & Controls

- □ Identify and list “Approved AI Tools” with owners and monitoring procedures.
- □ Define use cases that are permitted (e.g., enhancing productivity, summarization, code generation).
- □ Ensure tools are used in line with organizational values and existing policies.

Prohibited Users

- □ List prohibited behaviors (e.g., using AI for legal/HR/medical advice without human review, violating IP, etc).
- □ Add a section or table for “Prohibited AI Tools,” if applicable.

Data Responsibilities

- □ Require users to follow the data classification policy (e.g., no use of confidential/PII unless authorized).
- □ Enforce use of only approved data sources in prompts.
- □ Require encryption, access permissions, and secure storage to be managed by IT/security.

Employee Responsibilities

- □ Clearly state that users are accountable for all outputs generated using AI tools.
- □ Require that employees report any inappropriate AI usage or anomalies.
- □ Ensure training/awareness initiatives are available to support understanding and compliance.

AI Agent Use & Guardrails

- □ Require explicit approval by the AI Governance Team for any autonomous agents.
- □ Define mandatory safeguards: human-in-the-loop, override controls, and usage tracking.

Reporting, Exceptions, & Enforcement

- □ Include contact info for reporting violations or requesting exceptions (e.g., <Policy Owner>).
- □ Confirm a documented process exists for investigating incidents.
- □ Add a summary of disciplinary actions for non-compliance.

Review & Maintenance

- □ Assign a review lead and define the cadence (e.g., annual or quarterly).
- □ Maintain a revision history table with version, author, and description of changes.
- □ Ensure policy is approved by appropriate stakeholders and dated.