

INTERNAL AI POLICY TEMPLATE

This template should be modified to fit your specific organization as it governs the use of Artificial Intelligence (AI). Please review the template and edit as appropriate for the policies and procedures that are appropriate to protect your organization.



Scope

This policy applies to:

- All employees, contractors, and third-party vendors using AI tools or systems.
- All AI applications used across departments, including operations, HR, finance, marketing, and customer service.

Guiding Principles

We commit to using AI in ways that are:

- **Transparent:** Decisions made by AI must be explainable and documented.
- **Accountable:** Human oversight is required for all significant AI-driven decisions.
- **Fair:** AI systems must be monitored for bias and unintended consequences.
- **Secure:** AI tools must be protected from misuse or manipulation.
- **Compliant:** AI must follow all applicable laws, regulations, and internal policies.

Roles & Responsibilities

- **AI Governance Lead:** Oversees policy implementation, conducts audits, and reports findings to leadership.
- **Department Heads:** Ensure AI tools used in their teams follow this policy.

Roles & Responsibilities

- **IT Team:** Maintains infrastructure and security for AI systems.
- **Compliance Officer:** Monitors regulatory alignment and risk exposure.
- **All Users:** Must complete training and report concerns about AI behavior or outcomes.

Approved Use Cases

AI may be used for:

- Process automation (e.g., invoice processing, scheduling)
- Predictive analytics (e.g., customer behavior, inventory forecasting)
- Natural language processing (e.g., chatbots, sentiment analysis)
- Decision support (e.g., hiring recommendations, financial modeling)

Any use outside these areas requires written approval from the AI Governance Lead.

INTERNAL AI POLICY TEMPLATE

This template should be modified to fit your specific organization as it governs the use of Artificial Intelligence (AI). Please review the template and edit as appropriate for the policies and procedures that are appropriate to protect your organization.



Data Management

- **Training Data:** Must be accurate, relevant, and free from bias.
- **Sensitive Data:** AI systems must not process personally identifiable information (PII) or confidential business data unless explicitly authorized.
- **Data Retention:** AI-generated data must follow the organization's retention and disposal policies.

Risk Assessment & Auditing

Before deployment, all AI systems must undergo a **risk assessment** to evaluate:

- Accuracy and reliability
- Potential for bias or discrimination
- Security vulnerabilities
- Impact on users and stakeholders

Quarterly audits will be conducted to ensure ongoing compliance and performance.

Incident Response

If an AI system behaves unexpectedly or causes harm:

- Report the incident immediately to the AI Governance Lead.
- A root cause analysis will be conducted.
- Corrective actions may include system rollback, retraining, or deactivation.

Compliance & Enforcement

Violations of this policy may result in:

- Revocation of access to AI systems
- Disciplinary action
- Legal consequences if regulatory breaches occur

Review & Updates

This policy will be reviewed annually or when:

- New AI technologies are introduced
- Regulations change
- Significant incidents occur

Updates will be communicated to all stakeholders.