AI GOVERNANCE STARTER KIT

A Practical Guide to Governing AI Securely, Responsibly, and Effectively

ESTABLISH TRUST
Build confidence in AI use

REDUCE RISK
Strengthen security and compliance

DRIVE VALUE
Unlock AI's full potential

TEMPLATES
Ready-to-use artifacts

BEST PRACTICES
Proven governance models

STRATEGIC FRAMEWORKS
Implement with confidence

INTRO: HOW TO USE THIS PACKAGE

Purpose of This Package

This AI Governance Starter Kit is designed to help nonprofit organizations safely, responsibly, and compliantly begin adopting Artificial Intelligence (AI) technologies.

It includes:

- An **AI Acceptable Use Policy template**
- An **AI Risk Assessment**
- An **AI Readiness Assessment**

Together, these tools help organizations:

- Reduce risk
- Improve compliance posture (HIPAA, HITRUST, etc.)
- Establish governance before AI adoption expands

Who Should Use This

This package is intended for:

- Executive Leadership (CEO, COO, CFO)
- IT Administrators / MSPs
- Compliance & Privacy Officers
- HR Departments
- Board Members (for governance awareness)

How to Implement the AI Acceptable Use Policy

Step 1: Copy the Policy

- Copy the **AI Responsibility and Acceptable Use Policy** section into a Microsoft Word document.

Step 2: Replace Placeholder Text

- Use **Find and Replace (Ctrl + H)**
- Replace all instances of:
  [Company Name]
  with your organization's legal name.

Step 3: Review Internally

Have the document reviewed by:

- Executive leadership
- IT / Security
- Compliance / Legal (recommended)

Step 4: Add to Existing Policies

- Insert into:
  - Employee Handbook
  - Acceptable Use Policy (AUP)
  - Security Policy (if applicable)
-

Step 5: Communicate to Staff

- Distribute to all employees
- Require acknowledgment/signature
- Include in onboarding process

Important Note

This template is a starting point.
Each organization should review and adapt it to align with:

- Internal policies
- Legal requirements
- Compliance obligations

How to Use the Assessments

AI Risk Assessment

- Identifies **current exposure to AI-related risks**
- Helps uncover:
  - Shadow AI usage
  - Data exposure risks
  - Compliance gaps

AI Readiness Assessment

- Evaluates **how prepared your organization is to adopt AI safely**
- Helps define:
  - Next steps
  - Technology gaps
  - Governance maturity

SECTION 1: Artificial Intelligence (AI) Responsibility and Acceptable Use Policy

1. Purpose

This policy establishes guidelines for the responsible, ethical, and secure use of Artificial Intelligence (AI) tools within [Company Name]. As AI technologies become more accessible and embedded in everyday software, it is critical to ensure their use aligns with organizational values, data protection standards, regulatory requirements, and operational integrity.

This policy is designed to:

- Protect sensitive and regulated data, including Protected Health Information (PHI)
- Ensure compliance with HIPAA, HITRUST, and other applicable regulations
- Define acceptable and prohibited uses of AI
- Clarify employee responsibilities when using AI-generated content
- Reduce risks associated with data leakage, inaccuracies, and misuse of AI systems

2. Scope

This policy applies to all:

- Employees
- Contractors
- Volunteers
- Interns
- Third-party vendors with access to [Company Name] systems or data

It applies to all AI tools and platforms, including but not limited to:

- Chat-based AI (e.g., ChatGPT, Claude, Gemini, Copilot)
- AI features embedded in software (e.g., Microsoft 365, CRM systems, EHR platforms)
- AI transcription, summarization, and meeting tools
- AI-powered browser extensions or plugins
- Custom-built or internally deployed AI systems

AI Responsibility and Acceptable Use Policy

(Continued)

3. Definitions

Artificial Intelligence (AI):

Software systems capable of generating content, making predictions, summarizing information, or assisting in decision-making based on input data.

Protected Health Information (PHI):

Any information relating to an individual's health status, treatment, or payment for healthcare that can be linked to a specific individual, as defined under HIPAA.

Sensitive Data:

Includes, but is not limited to:

- PHI / ePHI
- Personally Identifiable Information (PII)
- Employee records
- Financial data
- Donor information
- Internal communications
- Security configurations
- Credentials and access information

Approved AI Tools:

AI systems that have been formally reviewed, approved, and provisioned by [Company Name] with appropriate security, compliance, and administrative controls.

4. Acceptable Use of AI

Employees may use AI tools **only under the following conditions**:

1. **Use of Approved Systems Only**
    - AI tools must be approved and provisioned by [Company Name].
    - Use must occur within company-managed environments and accounts.
2. **Appropriate Data Usage**
    - Only non-sensitive, non-confidential data may be used in AI tools unless explicitly authorized.
    - All use of sensitive data must follow approved workflows and controls.

AI Responsibility and Acceptable Use Policy

(Continued)

3. **Business Purpose**
    - AI may only be used for legitimate business purposes that align with job responsibilities.
4. **Human Oversight**
    - All AI-generated content must be reviewed, validated, and approved by the employee prior to use or distribution.

5. Prohibited Use of AI

The following activities are strictly prohibited:

1. **Use of Personal AI Accounts for Company Data**
    - Employees may not input [Company Name] data into AI tools accessed through:
        - Personal email accounts
        - Personal devices (unless explicitly authorized)
        - Unmanaged or non-company accounts
2. **Use of Unapproved AI Tools**
    - Employees may not use AI platforms that have not been reviewed and approved by [Company Name].
3. **Input of Sensitive or Regulated Data**
    - The following data must never be entered into unapproved AI systems:
        - PHI / ePHI
        - Client or patient information
        - Employee or HR records
        - Financial or accounting data
        - Donor or fundraising information
        - Internal reports, board materials, or strategic plans
        - System credentials or security configurations
4. **Circumventing Security Controls**
    - Employees may not bypass organizational safeguards to use AI tools.

6. HIPAA, HITRUST, and Regulatory Compliance

[Company Name] is subject to regulatory and compliance requirements, including but not limited to HIPAA and HITRUST.

- AI tools must not be used with PHI or regulated data unless:
    - The tool has been formally approved
    - Appropriate agreements (e.g., Business Associate Agreements) are in place
    - Security, privacy, and compliance controls have been validated

Unauthorized use of AI involving PHI may constitute a **reportable data breach** and may result in regulatory penalties.

AI Responsibility and Acceptable Use Policy

(Continued)

7. Data Privacy, Retention, and AI Memory Risks

Employees must understand that AI systems may:

- Store prompts and responses
- Retain uploaded files or data
- Use data to improve or train models (depending on the platform and settings)
- Maintain memory or personalization across sessions
- Log interactions for auditing or system improvement

Even if a user deletes a conversation:

- Data may still exist in system logs, backups, or vendor environments
- Information may persist in model behavior or memory features

Therefore:

Employees must assume that any data entered into an AI system **may be retained or exposed outside of [Company Name]'s control** unless the system is formally approved and governed.

8. Accuracy, Hallucinations, and Content Responsibility

AI systems can generate:

- Inaccurate or misleading information
- Fabricated data or "hallucinated" responses
- Outdated or biased content

Employee Responsibility:

- Employees are fully responsible for all content they generate using AI.
- AI-generated output must be:
    - Verified for accuracy
    - Reviewed for appropriateness
    - Confirmed against trusted sources

Prohibited Practices:

- Presenting AI-generated content as factual without verification
- Using AI to generate statistics, reports, or analysis without validating source data
- Relying on AI outputs for clinical, financial, legal, or compliance decisions without proper review

AI Responsibility and Acceptable Use Policy

(Continued)

9. AI Use in Reporting, Analytics, and Decision-Making

Employees must not:

- Use AI to fabricate or अनुमान data
- Present AI-generated statistics without supporting evidence
- Use AI outputs in official reports without validation

All AI-assisted outputs used in:

- Financial reporting
- Grant submissions
- Clinical documentation
- Board reporting

must undergo **formal review and validation**.

10. Security and Device Requirements

AI use must comply with [Company Name] security standards, including:

- Use of company-managed devices where required
- Multi-factor authentication (MFA)
- Endpoint protection
- Secure network access
- Compliance with IT and cybersecurity policies

Use of AI on personal or unmanaged devices is prohibited unless explicitly authorized.

11. Incident Reporting

Employees must immediately report:

- Unauthorized AI use involving company data
- Suspected data exposure or leakage
- Use of unapproved AI tools
- Any situation where sensitive data may have been entered into an AI system

Reports should be directed to:

- IT Department
- Compliance Officer
- Security Team
- Privacy Officer (as applicable)

AI Responsibility and Acceptable Use Policy

(Continued)

12. Monitoring and Enforcement

[Company Name] reserves the right to:

- Monitor AI tool usage within company systems
- Audit compliance with this policy
- Restrict or revoke access to AI tools
- Investigate potential violations

13. Disciplinary Action

Violation of this policy may result in:

- Loss of system access
- Disciplinary action, up to and including termination
- Legal action where applicable
- Regulatory reporting if required

14. Approved AI Governance

[Company Name] may provide approved AI tools and internally developed AI systems, including:

- Enterprise AI platforms
- Department-specific AI assistants (e.g., HR, Finance)
- Workflow-integrated AI tools

All approved AI tools will be:

- Configured with security and compliance controls
- Managed by IT and/or authorized personnel
- Subject to ongoing monitoring and governance

AI Responsibility and Acceptable Use Policy

(Continued)

15. Employee Acknowledgment

I acknowledge that I have read, understand, and agree to comply with the [Company Name] Artificial Intelligence (AI) Responsibility and Acceptable Use Policy.

I understand my responsibilities regarding:

- Data protection
- Proper use of AI tools
- Verification of AI-generated content
- Reporting of incidents or misuse

I understand that failure to comply with this policy may result in disciplinary action.

Employee Name: _____

Signature: _____

Date: _____

SECTION 2: AI RISK ASSESSMENT TEMPLATE

Purpose

To identify and evaluate risks associated with current or potential AI usage within [Company Name].

Instructions

For each category:

- Rate Risk Level: **Low / Medium / High**
- Provide notes
- Identify mitigation actions

AI Risk Assessment Table

Category	Risk Description	Risk (L/M/H)	Current State	Mitigation Plan
Shadow AI Usage	Employees using AI tools without IT approval			
Personal Device Usage	AI accessed via personal laptops or mobile devices			
Unapproved AI Platforms	Use of tools like ChatGPT, Claude, Gemini outside governance			
PHI / ePHI Exposure	Sensitive healthcare data entered into AI tools			
Employee Data Exposure	HR or personnel data used in AI systems			
Financial Data Exposure	Budgets, reports, or accounting data used in AI			
Donor / Client Data Exposure	Confidential donor or client data shared with AI			
Data Retention Risk	AI tools storing or retaining submitted data			
AI Hallucinations	AI generating false or misleading information			
Unverified AI Outputs	Staff using AI-generated content without validation			
Regulatory Compliance Risk	Violations of HIPAA, HITRUST, or privacy laws			
Lack of AI Policy	No formal governance or acceptable use policy			
Lack of Training	Employees unaware of AI risks			
Vendor Risk	AI vendors lacking proper agreements/security			
Reputational Risk	Public-facing errors caused by AI			

Overall Risk Summary

- **Total High Risks:** _____
- **Key Areas of Concern:** _____
- **Immediate Actions Required:** _____

SECTION 3: AI READINESS ASSESSMENT

Purpose

To evaluate [Company Name]'s ability to safely adopt and scale AI technologies.

Scoring System

Score	Meaning
1	Not In Place
2	Minimal / Informal
3	Defined but inconsistent
4	Implemented and managed
5	Mature and optimized

Assessment Categories

1. Governance & Policy

Question	Score (1–5)
AI Acceptable Use Policy exists	
AI usage is formally approved by leadership	
AI governance roles are defined	
AI risk management process exists	

3. Security & Compliance

Question	Score (1–5)
AI tools are evaluated for HIPAA/HITRUST compliance	
Data classification is implemented	
DLP (Data Loss Prevention) policies exist	
MFA and access controls enforced	

2. Technology & Tools

Question	Score (1–5)
Approved AI platforms are defined	
Microsoft 365 environment is secured and configured	
Endpoint/device management is in place	
Logging and monitoring are enabled	

4. Data Management

Question	Score (1–5)
Sensitive data is classified and labeled	
Access to data is properly controlled	
Data retention policies exist	
Data sharing policies are enforced	

Assessment Categories

(Continued)

5. User Awareness & Training

Question	Score (1–5)
Employees are trained on AI risks	
AI usage guidelines are communicated	
Staff understand PHI restrictions	
Ongoing training program exists	

6. Operational Readiness

Question	Score (1–5)
AI use cases are defined (HR, Finance, etc.)	
AI outputs are reviewed/validated	
AI is integrated into workflows responsibly	
Leadership supports structured AI adoption	

Scoring Summary

- **Total Score:** _____ / 100
- **Maturity Level:**
  - 0–30 → High Risk / Not Ready
  - 31–60 → Developing
  - 61–80 → Moderately Ready
  - 81–100 → AI Ready

Recommended Next Steps

Based on your score:

- **Low Score:**
  Establish governance and policy immediately

- **Mid Score:**
  Implement approved tools and controls

- **High Score:**
  Begin structured AI deployment and optimization

ABOUT THIS RESOURCE

This Non-Profit AI Governance Starter Kit was created to help organizations:

- **Navigate AI adoption safely**
- **Protect sensitive data**
- **Maintain compliance**
- **Enable innovation responsibly**

Powered By

Managed IT Services & Solutions for Nonprofits
New York / Long Island
www.allsector.com

Supporting nonprofits with:

- Technology guidance
- Security best practices
- Digital transformation resources

www.center4.com

Disclaimer

This document is provided for informational purposes only and should be reviewed by legal and compliance professionals before implementation.