HELPING BUSINESSES ACHIEVE MEASURABLY BETTER IT®

TEMPLATE FOR PUBLIC USE

AI Acceptable Use & Governance Policy

PURPOSE

This policy defines how Artificial Intelligence (AI) tools may be used within the organization to improve productivity and innovation without increasing risk. It establishes guardrails to protect sensitive data, intellectual property, regulatory obligations, and client trust.

Our goal is clarity and confidence: AI should support decision-making and operations, not replace accountability or introduce unmanaged risk.

SCOPE

This policy applies to:

- All employees, contractors, and temporary staff
- All AI-enabled tools, platforms, assistants, and integrations
- All use of AI for business, client, operational, or marketing purposes

GUIDING PRINCIPLES

AI use within the organization must be:

- **Secure** – Protecting confidential, regulated, and proprietary information
- **Compliant** – Aligned with applicable laws, regulations, and contractual obligations
- **Transparent** – Understandable and explainable to stakeholders
- **Accountable** – Humans remain responsible for decisions and outcomes
- **Measurable** – Delivering clear business value with managed risk

AI Acceptable Use & Governance Policy

1. Acceptable Use Guidelines

Permitted Uses

AI tools may be used for:

- Drafting, summarizing, and editing non-confidential content
- Brainstorming ideas, outlines, and first-pass concepts
- Research on public or approved internal information
- Data analysis using approved, sanitized datasets
- Automating repetitive tasks with documented oversight

All outputs must be reviewed and validated by a human before use in:

- Client-facing communications
- Operational decisions
- Financial, legal, or compliance-related activities

Prohibited Uses

AI tools must not be used for:

- Entering or processing sensitive, confidential, or regulated data
- Making autonomous decisions affecting clients, finances, security, or compliance
- Replacing required professional judgment (legal, financial, medical, security)
- Circumventing internal controls, approvals, or audit processes
- Training public AI models with company or client data

2. Data Handling & Confidentiality

Data Classification Rules

The following data must never be entered into AI tools unless explicitly approved:

- Client data or personally identifiable information (PII)
- Protected health information (PHI)
- Financial records or payment information
- Authentication credentials or security configurations
- Internal proprietary processes, pricing, or intellectual property

Approved Data Usage

Only the following data types may be used:

- Publicly available information
- De-identified or anonymized datasets
- Content explicitly approved for AI processing

Retention & Logging

- AI interactions involving business data should be logged where supported
- Outputs used for decision-making must be retained according to record retention policies
- No AI-generated content should be assumed accurate without verification

3. Vendor & Tool Approval Guardrails

Approved AI Tools
Only AI tools that have completed a security and compliance review may be used for business purposes.
Approval criteria include:

- Data handling and retention policies
- Security controls and encryption standards
- Compliance alignment (HIPAA, GDPR, SOC2, etc., as applicable)
- Transparency on model training and data usage
- Vendor stability and support

Unapproved Tools

- Free, consumer-grade AI tools are not approved by default
- Browser extensions or plugins using AI must be reviewed
- Personal AI accounts may not be used for business data

Review Process

- All new AI tools require approval from IT / Security leadership
- Periodic re-evaluation of approved tools will be conducted
- High-risk or regulated use cases require documented governance approval

4. Human Oversight & Accountability

- AI outputs are advisory only
- Employees remain fully responsible for accuracy and outcomes
- Decisions impacting clients, compliance, or security require human validation
- Errors or unintended consequences must be reported immediately

AI does not remove accountability.

5. Training & Awareness

- Employees must complete AI awareness training before using approved tools
- Training will cover:
    - Appropriate use cases
    - Data protection expectations
    - Risk awareness (hallucinations, bias, over-reliance)
- Ongoing education will evolve with AI capabilities and regulations

6. Monitoring & Enforcement

- AI usage may be monitored to ensure compliance
- Violations may result in:
    - Revocation of AI access
    - Disciplinary action
    - Legal or contractual consequences

7. Policy Review & Updates

This policy will be reviewed:

- At least annually
- Upon major regulatory changes
- When introducing new AI capabilities or vendors

Updates will be communicated clearly to all staff.

3. Vendor & Tool Approval Guardrails

Approved AI Tools
Only AI tools that have completed a security and compliance review may be used for business purposes.
Approval criteria include:

- Data handling and retention policies
- Security controls and encryption standards
- Compliance alignment (HIPAA, GDPR, SOC2, etc., as applicable)
- Transparency on model training and data usage
- Vendor stability and support

Unapproved Tools

- Free, consumer-grade AI tools are not approved by default
- Browser extensions or plugins using AI must be reviewed
- Personal AI accounts may not be used for business data

Review Process

- All new AI tools require approval from IT / Security leadership
- Periodic re-evaluation of approved tools will be conducted
- High-risk or regulated use cases require documented governance approval

4. Human Oversight & Accountability

- AI outputs are advisory only
- Employees remain fully responsible for accuracy and outcomes
- Decisions impacting clients, compliance, or security require human validation
- Errors or unintended consequences must be reported immediately

AI does not remove accountability.

5. Training & Awareness

- Employees must complete AI awareness training before using approved tools
- Training will cover:
  - Appropriate use cases
  - Data protection expectations
  - Risk awareness (hallucinations, bias, over-reliance)
- Ongoing education will evolve with AI capabilities and regulations

6. Monitoring & Enforcement

- AI usage may be monitored to ensure compliance
- Violations may result in:
  - Revocation of AI access
  - Disciplinary action
  - Legal or contractual consequences

7. Policy Review & Updates

This policy will be reviewed:

- At least annually
- Upon major regulatory changes
- When introducing new AI capabilities or vendors

Updates will be communicated clearly to all staff.