DIGITAL FIRE.CA
MANAGED TECHNOLOGY

AI Acceptable Use & Governance Policy

Protect your business, streamline operations, and leverage AI with confidence.

Artificial Intelligence (AI) is transforming the way organizations operate, offering opportunities to enhance productivity, streamline processes, and drive innovation. However, with great power comes great responsibility. This AI Acceptable Use & Governance Policy Template is designed to help organizations implement AI responsibly, ensuring compliance, security, and accountability while fostering trust with stakeholders.

This policy template provides a comprehensive framework for organizations to govern the use of AI tools effectively. It establishes clear guidelines to protect sensitive data, maintain regulatory compliance, and ensure that AI serves as a tool for progress without introducing unmanaged risks.

DIGITAL FIRE.CA
MANAGED TECHNOLOGY

Scope

This policy applies to:

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

Guiding Principles

The responsible use of AI within an organization is guided by the following principles:

- **Security:** Safeguard confidential, regulated, and proprietary information.
- **Compliance:** Align with applicable laws, regulations, and contractual obligations.
- **Transparency:** Ensure AI processes and outputs are understandable and explainable.
- **Accountability:** Retain human responsibility for decisions and outcomes.
- **Measurability:** Deliver clear business value while managing risks effectively.

1 Acceptable Use Guidelines

Permitted Uses

AI tools may be used for:

- Drafting, summarizing, and editing non-confidential content.
- Brainstorming ideas, creating outlines, and developing first-pass concepts.
- Conducting research on publicly available or approved internal information.
- Analyzing data using pre-approved, sanitized datasets.
- Automating repetitive tasks under documented oversight.

All AI-generated outputs must be reviewed and validated by a human before being used in client-facing communications, operational decisions, or financial/legal activities.

Prohibited Uses

To ensure data security, AI tools **must not** be used for:

- Entering or processing sensitive, confidential, or regulated data.
- Making autonomous decisions that affect clients, finances, security, or compliance.
- Replacing required professional judgment (e.g., legal, financial, medical, or security assessments).
- 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 types of data must never be entered into AI tools unless explicitly approved:

- Client data or Personal Information, as defined under PIPEDA and applicable provincial privacy legislation.
- Personal Health Information, as defined under applicable provincial health information legislation (e.g., PHIPA in Ontario).
- Financial records or payment information.
- Authentication credentials (passwords, API keys) 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 fully anonymized datasets.
- Content explicitly approved for AI processing.

Digital Fire recommends vetting tools based on data retention policies, encryption standards, and compliance alignment (e.g., HIPAA, SOC2)

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.

DIGITAL FIRE
MANAGED TECHNOLOGY

3 Vendor & Tool Approval

Only AI tools that have undergone a thorough security and compliance review may be used for business purposes.

Approval criteria include:

- Robust data handling and retention policies.
- Advanced security controls and encryption standards.
- Compliance with regulations such as HIPAA, GDPR, and SOC2, etc., as applicable.
- Transparency regarding model training and data usage.
- Vendor stability and ongoing support.

Unapproved Tools ("Shadow AI")

- **Free, consumer-grade AI tools** are not approved by default.
- **Browser extensions or plugins** utilizing AI must undergo review before installation.
- **Personal AI accounts** may not be used for business data processing.

Review Process

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

NEED HELP
VETTING A TOOL?

Call Us: 905-845-5959

4 Human Oversight & Accountability

AI does not remove accountability.

- AI outputs are advisory and must not replace human judgment.
- Employees remain fully responsible for the accuracy and outcomes of AI-assisted decisions.
- Decisions impacting clients, compliance, or security require human validation.
- Any errors or unintended consequences must be reported immediately.

5 Training & Awareness

To ensure responsible AI use, all employees must complete AI awareness training before using approved tools.

Training will cover:

- Appropriate use cases for AI.
- Data protection expectations.
- Risks associated with AI, such as hallucinations, bias, and over-reliance.

Ongoing education will evolve alongside advancements in AI capabilities and regulatory changes.

6 Monitoring & Enforcement

Organizations may monitor AI usage to ensure compliance with this policy. Violations may result in:

- Revocation of AI access.
- Disciplinary action.
- Legal or contractual consequences.

Policy Review
This policy will be reviewed at least annually, or upon major regulatory changes or the introduction of new AI capabilities.

DIGITAL FIRE
MANAGED TECHNOLOGY

DIGITAL FIRE.CA
MANAGED TECHNOLOGY

SECURE YOUR ORGANIZATION'S FUTURE WITH AI GOVERNANCE

AI's power is undeniable, but **unchecked use poses significant risks.** Without immediate action, your organization faces potential reputational damage, security breaches, and legal non-compliance. Do not let innovation become a liability. **Act now** to ensure responsible AI implementation.

IMPLEMENT THIS POLICY IMMEDIATELY. This AI Acceptable Use & Governance Policy Template is your essential tool to establish critical guidelines today. Empower your team to harness AI's potential safely and effectively, before it's too late. Secure trust, maintain compliance, and drive progress responsibly.

Act now with expert support — contact us to ensure responsible AI governance.

Call Us: 905-845-5959

905-845-5959 | www.digitalfire.ca | info@digitalfire.ca