AI Policy Template

Version: 1.0 (Starter Policy)

Mapped to:
Lecture 10.1 – *Your Week 1 Action Checklist*

Purpose:
This policy establishes clear, practical, and enforceable guidelines for the responsible use of Artificial Intelligence (AI) within the organization. It is designed to enable fast AI adoption **without compromising security, compliance, ethics, or trust**.

This is a **living document** and should evolve as AI capabilities, regulations, and business use cases mature.

---

1. POLICY OBJECTIVES

The objectives of this AI Policy are to: - Enable safe, ethical, and productive use of AI tools - Protect confidential, personal, and regulated data - Ensure compliance with legal and regulatory obligations - Clarify accountability and decision ownership - Promote transparency and responsible innovation

---

2. SCOPE OF THE POLICY

This policy applies to: - All employees, contractors, consultants, and interns - All departments and business units - All AI tools, platforms, and services used for business purposes

This includes, but is not limited to: - Generative AI tools (text, image, code, audio) - Embedded AI features in enterprise software - Custom-built AI systems - Third-party AI services

---

3. DEFINITIONS

- **Artificial Intelligence (AI):** Systems that perform tasks requiring human-like intelligence such as reasoning, content generation, prediction, or decision support.
- **Generative AI:** AI models that generate text, images, code, audio, or video based on prompts.
- **AI Output:** Any content, recommendation, or decision produced by an AI system.
- **Sensitive Data:** Confidential, personal, financial, health, or regulated information.

---

4. GUIDING PRINCIPLES

All AI use within the organization must follow these principles:

1. **Human Accountability:** AI supports decisions; humans remain accountable.
2. **Transparency:** AI use should be disclosed where appropriate.
3. **Data Protection:** Sensitive data must never be exposed unnecessarily.
4. **Fairness:** AI must not be used to discriminate or bias decisions.
5. **Security by Design:** AI systems must meet security standards.

---

5. APPROVED AI USE CASES

AI may be used for: - Drafting and summarizing documents - Research and information synthesis - Data analysis and reporting support - Customer service assistance (with safeguards) - Software development assistance

All new AI use cases must be reviewed and approved as per Section 12.

---

6. PROHIBITED AI USE CASES

AI must NOT be used for: - Final legal, medical, or financial decisions without human review - Autonomous decision-making affecting employment, credit, or legal rights - Uploading confidential or personal data into unapproved tools - Surveillance or employee monitoring without legal approval - Generating deceptive, misleading, or false information

---

7. DATA HANDLING & PRIVACY

7.1 Data Classification

Employees must classify data before using AI: - Public - Internal - Confidential - Restricted

Only **Public** and **Internal** data may be used with approved AI tools unless explicitly authorized.

7.2 Personal Data

Personal data must be: - Minimized - Anonymized or masked where possible - Used in compliance with applicable privacy laws

---

8. SECURITY REQUIREMENTS

All AI tools must: - Be approved by IT and Security - Meet organizational security standards - Support access controls and logging - Prevent unauthorized data retention or reuse

Employees must not use personal AI accounts for business data.

---

9. AI OUTPUT VALIDATION

- AI-generated content must be reviewed by a human before use
- Outputs must be verified for accuracy, bias, and appropriateness
- AI outputs must not be treated as facts without validation

---

10. INTELLECTUAL PROPERTY & COPYRIGHT

- Employees are responsible for ensuring AI outputs do not infringe IP rights
- Proprietary data must not be used to train external AI models unless approved
- Ownership of AI-generated content follows existing IP policies

---

11. ETHICAL USE & BIAS MITIGATION

The organization commits to: - Monitoring AI systems for bias - Avoiding discriminatory outcomes - Escalating ethical concerns immediately

Any suspected unethical AI use must be reported.

---

12. GOVERNANCE & APPROVAL PROCESS

12.1 AI Governance Committee

Responsibilities include: - Approving AI tools and use cases - Monitoring risks and compliance - Updating this policy

12.2 New Use Case Approval

New AI use cases must include: - Business objective - Data used - Risk assessment - Owner accountability

---

13. TRAINING & AWARENESS

- All employees must complete basic AI awareness training
- Role-based training will be provided where required
- Policy updates will be communicated formally

---

14. INCIDENT MANAGEMENT

AI-related incidents include: - Data leakage - Incorrect or harmful AI output - Security breaches

All incidents must be reported immediately and investigated.

---

15. MONITORING, AUDIT & ENFORCEMENT

- AI usage may be monitored for compliance
- Violations may result in disciplinary action
- Regular audits will be conducted

---

16. POLICY REVIEW & UPDATES

This policy will be reviewed: - At least annually - After major regulatory or technological changes

---

17. ACKNOWLEDGEMENT

All employees must acknowledge understanding and compliance with this policy.

Final Note:
This policy is designed to **enable AI adoption, not slow it down**. Responsible AI use is a leadership responsibility, not just a technical one.