Premier One

Artificial Intelligence (AI) Best Practices Policy

Effective Date: [Insert Date]
Applies To: All Employees, Contractors, and Vendors
Approved By: [Insert Approving Authority or Committee Name]

---

1. Purpose

This plan establishes detailed guidelines for the responsible, ethical, and secure use of Artificial Intelligence (AI) technologies within [Company Name]. It aims to mitigate risks related to data privacy, intellectual property, regulatory exposure, and ethical concerns while maximizing the operational, strategic, and innovative benefits of AI adoption.

---

2. Scope

This policy applies to: - All employees and contractors who interact with AI tools in any capacity. - Third-party partners or vendors whose services include the use or deployment of AI on behalf of [Company Name]. - AI systems including, but not limited to: generative AI (text, image, audio), machine learning models, natural language processing systems, predictive analytics, and decision-support systems.

---

3. Core Principles

- **Ethics and Responsibility:** All AI usage must prioritize fairness, transparency, non-discrimination, and respect for human rights. AI must never be used to deceive, mislead, or exploit individuals.
- **Data Security:** All data processed by AI systems must follow internal classification and encryption policies. Only de-identified data should be used for non-secure environments.
- **Compliance:** AI-related activities must comply with GLBA, ALTA, FFIEC, and applicable federal/state data privacy regulations.
- **Risk Management:** Evaluate the downstream consequences of AI use—technically, reputationally, and operationally.
- **Human Review:** AI-generated content, recommendations, or decisions must be reviewed and approved by a qualified employee. This includes documents, client communications, loan decisions, marketing copy, and risk scoring.

---

4. Data Privacy and Security

4.1 Personal Information - **Strict Prohibition:** Employees must not enter any non-public customer information (NPI), PII, PHI, or bank account data into public AI tools. - **Permissible Tools:** Only use AI tools that meet compliance thresholds (e.g., SOC 2 Type II, ISO 27001) for handling personal or regulated data. - **Audit Trails:** Maintain records of data inputs and outputs for sensitive use cases to ensure traceability.

4.2 Proprietary Information - **Restricted Content:** Never share legal documents, underwriting methodologies, financial models, or transaction data with AI platforms lacking contractual data protections. - **Review Process:** Any AI-generated content used externally (e.g., client emails, marketing material) must undergo documented human review. - **Watermarking:** When feasible, flag AI-generated content for internal reference and compliance auditing.

---

5. Licensing and Accountability

5.1 Paid AI Subscriptions - **Designated Licensee:** All AI accounts must be registered under a corporate domain with a designated administrator. - **Usage Logs:** Maintain access and activity logs for accountability and audits. - **Tool Inventory:** IT must maintain a list of authorized AI tools and their intended business use.

5.2 Contractual Safeguards - **Data Handling Clauses:** Contracts must specify data ownership, retention, deletion protocols, and that vendor models will not be trained using company data. - **Performance Benchmarks:** Include SLAs to define acceptable AI output quality and response times.

---

6. Governance and Oversight

6.1 AI Governance Committee - Comprised of representatives from Legal, Compliance, IT Security, and business leaders. - Responsible for: - Evaluating new AI vendors and tools. - Approving high-risk AI use cases. - Updating the AI policy based on regulatory changes.

6.2 Employee Training - **Curriculum:** Annual training covering AI ethics, data entry rules, risk examples, incident reporting, and legal implications. - **Department-Specific Training:** Tailored content for sales, underwriting, IT, HR, and marketing.

6.3 Risk Assessment - Assess: - Risk of biased or inaccurate output. - Legal exposure in automated workflows. - Regulatory red flags in client-facing tools.

---

7. Ethical AI Use

- **Bias Testing:** Perform regular fairness assessments and blind validation tests on models.
- **Disclosure Statements:** When AI tools affect client decisioning, disclose that AI was used, and provide a path to human review.
- **Decision Boundaries:** Never allow AI to make final underwriting or legal conclusions without secondary human approval.

---

8. Incident Response and Monitoring

- **Real-Time Alerts:** Monitor AI system behaviors for anomalies, hallucinations, or unsanctioned data exposure.
- **Incident Reporting Channel:** All users must immediately report suspected AI misuse to Compliance.
- **Review Timeline:** Incident root cause analysis must occur within 2 business days.

---

9. Vendor Management

- **Security Vetting:** Before adoption, vendors must submit independent third-party audits (SOC 2, penetration tests, etc.).
- **Ongoing Assessment:** Re-assess vendors annually for operational, compliance, and reputational risks.
- **Termination Protocols:** Ensure prompt offboarding and data deletion upon contract termination.

---

10. Implementation and Review

- **Rollout Checklist:** Establish milestones for department compliance, training completions, and tool inventory.
- **Annual Review:** The policy and related procedures must be reviewed and updated annually or when laws change.
- **Feedback Loop:** All employees are encouraged to report inefficiencies or risks in current AI workflows.

---

11. Legal and Regulatory Considerations (Title Insurance and Banking)

11.1 Industry-Specific Compliance Requirements - **Title Insurance:** - ALTA Best Practices Framework v4.0 (or most current) - State Department of Insurance (DOI) guidelines - CFPB oversight for consumer data protection - Gramm-Leach-Bliley Act (GLBA) for safeguarding consumer information

- **Banking and Financial Services:**
  - FFIEC Guidance on AI and Automated Systems (as published)
  - Federal Reserve and OCC risk management expectations
  - Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) regulations
  - FDIC and NCUA data protection requirements

11.2 Compliance Documentation and Audits - Retain records of: - Tool evaluations and vendor risk assessments. - Staff training logs. - Risk mitigation measures. - Usage audits by department.

11.3 Use Case Approval - Mandatory for any application involving: - Loan approvals or escrow workflows - Financial calculations for client accounts - Email or communications impersonation detection

11.4 Data Localization and Jurisdiction - All data processing must occur on U.S.-hosted servers unless explicitly approved by Legal and Security. - Tools involving international teams or APIs must comply with GDPR, UK DPA, or similar frameworks.

---

12. Acknowledgement and Sign-Off

All employees and contractors must acknowledge their understanding and compliance with this policy annually.

Employee Acknowledgement
Name: _____
Signature: _____
Date: _____

Manager Acknowledgement (Responsible for Department Compliance)
Manager Name: _____
Signature: _____
Department: _____
Date: _____

Document Control
Version: 1.0
Last Reviewed: [Insert Date]
Next Review Date: [Insert Date]
Owner: [Insert Policy Owner or Department Name]