NBA / NBAF Innovation Committee

IMPLEMENTING A COPORATE WIDE AI POLICY IN THE AGE OF AI

August 1st, 2025

National Bankers Association Foundation

Why have an AI Corporate Policy in the Age of AI?

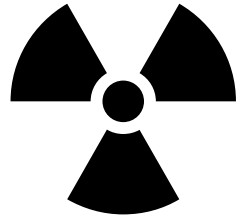
Why is a Corporate AI Policy Important?

National Bankers Association Foundation

Data Security

Financial Regulations

Financial Inclusion



Risk Management

AI Policy an Enabler of Data Security

National Bankers Association Foundation

- **Establishes Control** over Data Management and Access Within Your Organization
  - Imperative when third party vendors require access to customer financial data
  - Establish infrastructure to control access to customer financial data
- **Guides Staff** Training and Day-to-Day Operation Around Customer Data Privacy and Security
- **Creates Protocols for Audits** and Transparency on the Use of AI with Customer Data
  - Flags unauthorized access and practices
- **Scopes Remedial Procedures** in Cases of Eventual Data Breaches

Compliance with Financial Regulations

National Bankers Association Foundation

- Consumer Financial Protection Bureau (CFPB)*
  - Applications involving lending
  - Consumer facing applications like chatbots

cfpb Consumer Financial Protection Bureau

- Financial Industry Regulatory Authority (FINRA)**
  - Issued guidance on use of AI by financial institutions especially banks
  - AI policy strongly recommended by FINRA in latest guidance

FINRA

- Gramm-Leach-Bliley Act ***
  - Banking regulation that covers consumer data privacy and security
  - Enforced by Federal Trade Commission (FTC)

* https://www.consumerfinance.gov/about-us/blog/cfpb-has-entered-the-chat/
https://bankingjournal.aba.com/2024/08/cfpb-to-crack-down-on-bank-chatbots/

** https://www.finra.org/rules-guidance/key-topics/fintech/report/artificial-intelligence-in-the-securities-industry/key-challenges

***https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

AI Policy an Agent for Financial Inclusion

National Bankers Association Foundation

- A Corporate AI Policy allows for Executive Board Level Ethical Concerns to be Addressed
- AI Policy Should Ensure a Safe, Fair and Compliant AI Utilization including input, consultation and approval from Executive Board Members
- An AI Policy Helps to Combat Against Bias in AI's Customer Decisioning for Financial Institutions Providing Services to Ethnic Minorities
- An AI Policy Helps Emphasize An Organizational Wide adoption of Financial Inclusion Themes In Their Utilization Of AI Technology Financial Service

Risk Management Best Practice

National Bankers Association Foundation

- Developing a Corporate AI Policy Is Recommended Best Practice for Risk Management for Financial Institutions

- National Institute of Standards and Technology (NIST) Has Developed an AI Risk Management Framework (RMF) That Is Recommended to Banks to Help Manage The Risks That They Are Exposed to In Their Utilization Of AI for Their Operations *

- Most AI tools Are Provided by External Third-Party Vendors, Thus, Necessitating The Need For Policies That Guide The Integration of These Third-party Vendors

- Certain Artificial Intelligence Applications Can Introduce Regulatory and Operational Risks Which Need to be Mitigated

* https://www.nist.gov/itl/ai-risk-management-framework

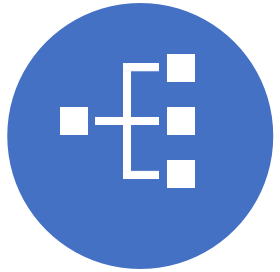
Elements of an AI Corporate Policy

Elements of a Corporate AI Policy

National Bankers Association Foundation

AI OFFICER/ PERSONNEL

TERMINOLOGY DEFINITIONS



ORGANIZATION CONTROLS

SAFETY & AUDIT CONTROLS

ETHICAL CONSIDERATIONS

ACCEPTABLE USE CASES

THIRD PARTY RISK CONTROLS

Defining an AI Officer Role

National Bankers Association Foundation

RESPONSIBILITIES

- Coordination of Staff Training On AI Use
- Risk Assessment of New Vendors And AI Applications
- Regulatory Risk Assessment of AI Applications
- Point of Report for AI Incidents Especially with New Vendor AI Tools or Other AI Applications
- Crafts AI Strategy And Goals of Organization
  - Why Are We Using AI?
  - What Do We Want To Accomplish?
- Updates Organization on Latest News And Development On AI Use

Establishing Definitions of Terminologies

National Bankers Association Foundation

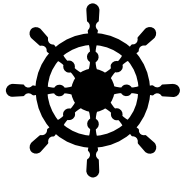
TERMINOLOGIES

- List All Terminologies & Jargons Used In Corporate AI Policy
- Clearly Define Each Listed Terminology. Avoid Using Technical Terms in Terminology Description
- Give Examples to Explain Terminologies Where Necessary
- Refer to Terminologies Where Necessary in the Body of AI Policy for Easy Readership and Understanding
- Reference External Resources to Provide Further Information on Terminologies, Especially Technical Jargons

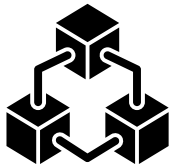
Organization Control & Mapping

National Bankers Association Foundation

A Mapping of Bank Operations Impacted by AI Technology and Its Interconnectedness



Delineation of Control Measures/Stops Gaps To Deactivate AI Technology & Contain Impact Spread in Case of an Incidence



Back-Up Protocol to Operate without AI Technology

Remedial Actions & Strategies In Event of Incidence – Incidence Plan & Disaster Recovery Plan

Safety Controls

National Bankers Association Foundation

SAFE OPERATIONS

- List of AI platforms and Infrastructure That Can be Used by Staff
- Data Privacy Considerations for ChatGPT Like Tools and AI Third Party Vendors
- Controls on Data Entry into ChatGPT /AI platforms

There are custom tools that flag/auto-redact personal identifiable information (PII) when typed into AI tools

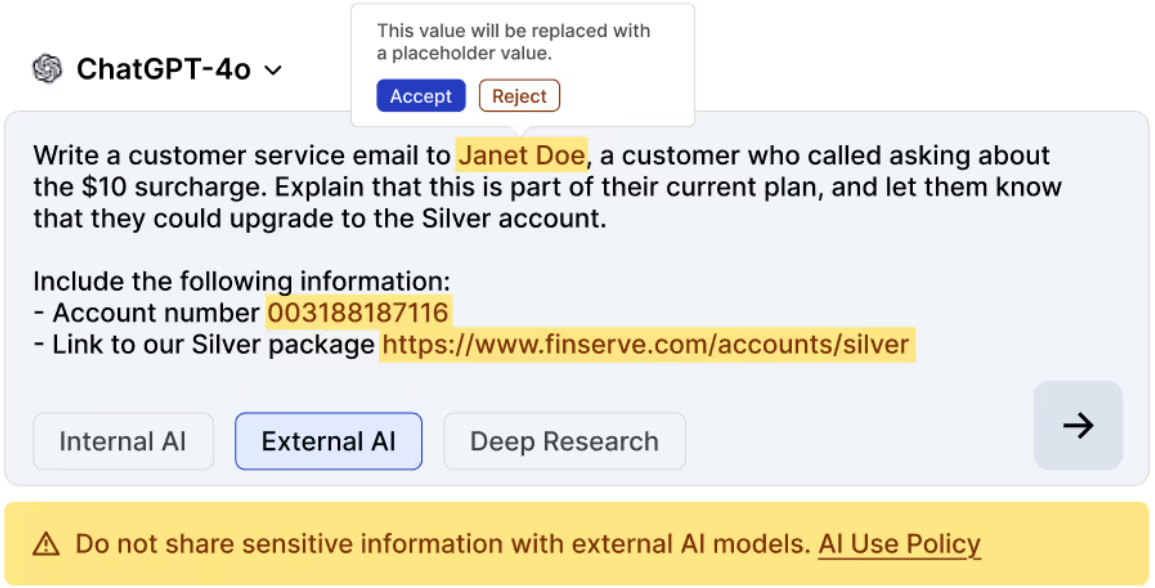


Image Source: *userfront*

Audit Controls

National Bankers Association Foundation

CONTROLS & LOGS

- Information Security Requirements
  - Standard Cybersecurity Policies
- Establishment of AI Activity Logging System
- Authentication & Login Protocols
  - Staff login required for all AI-Tools
  - Allows for easy audit – Who did what?
- Role-based Data Access & Functionality Control

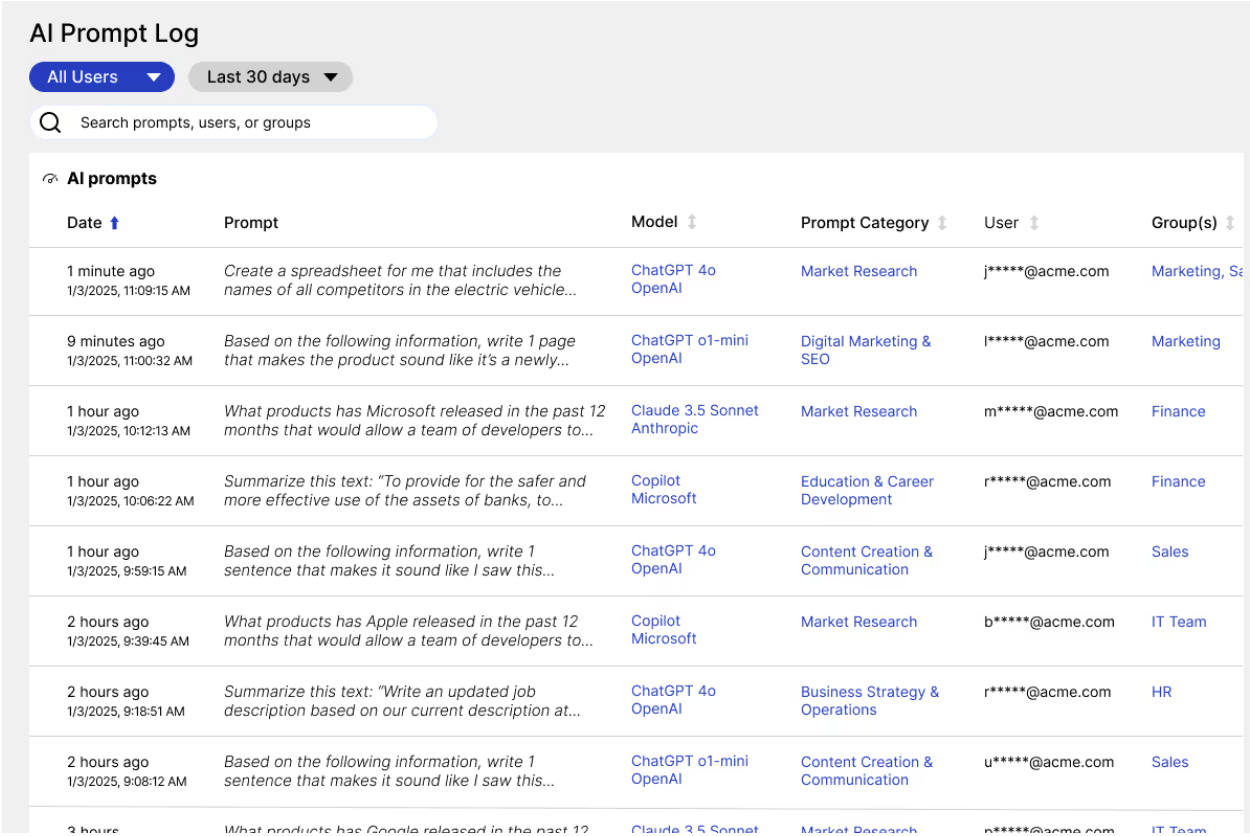


Image Source: *userfront*

Ethics in the Age of AI

National Bankers Association Foundation

AI GOVERNANCE

- Policies Should Ensure a Safe, Fair and Compliant AI Utilization
- Align AI Operational Framework & Applications to Organizational Values and Regulatory Themes

  Thorough and Clear Understanding of AI Use Case across Departments and Their Interconnectedness
  Understanding AI Talent Recruitment
- Ethical and Value Alignment with AI Third-Party Vendors
- Establish Framework for Staff to Report Ethical Concerns with AI Applications

Acceptable Use Cases

National Bankers Association Foundation

USE-CASES

- Clearly Delineate and Give Examples of Acceptable Use Cases
  - Describe Overarching Doctrine Guiding Acceptable Use Cases
- Also Delineate Forbidden Use Cases and Provide Examples
- Establish Protocol for Ascertaining if an Application Is an Acceptable Use
  - Intake Forms Submitted to AI Officer for Reviewing New Use Cases
  - Protocol for Staff to Seek Clarity on New Use Cases
- Document Consequences for Acceptable Use-Case Violations

Third-Party Risk Management Controls

National Bankers Association Foundation

SECURITY MEASURES

- Certifications Required of Third-Party Vendors
  - SOC I, SOC II and ISO/IEC 27001
- Security Tests Required of Third-Party Vendors
  - List of Types of Tests – E.g. Penetration Testing, Vulnerability Scan, etc.
  - Required Periodic Schedule for these Tests
- Third-Party Vendor Audit Requirements & Audit Schedule
- Policy on Data Storage
  - Determining Whether to Host In-House, or Trusting Vendor's Cloud Infrastructure
  - Determining Critical/Non-Critical Operations:
    - When Can Data Leave the Bank Infrastructure?
    - When Can Data be Hosted in Third Party Environment?

SUMMARY

National Bankers Association Foundation

- The organization is advised to designate an AI Officer responsible for coordinating AI training, overseeing risk assessments, managing vendor relationships, monitoring AI incidents, and updating the organization on AI developments.
- Safety controls are recommended, including restricting staff to approved AI platforms, enforcing data privacy and cybersecurity protocols, and managing information flow to online AI tools like ChatGPT and vendor solutions.
- Audit protocols should cover information security, authentication, and role- based data access controls to ensure robust oversight of AI systems.
- The committee stressed the importance of ethical AI use—establishing safe, fair, and compliant practices, auditing stakeholder readiness, and building internal champions to drive long-term trust and adoption.

Open Discussion & Closing