AI Policy Template for Finance (2025) — Governance, Controls & Examples

Publication-ready template with jurisdictional references, governance controls, data handling, QC blocks, and auditor-friendly mapping

Quick Summary

- Copy-ready finance AI policy with clear scope, allowed use cases, and QC blocks.
- Includes country/standard references: GDPR, DPDP Act 2023, CCPA/CPRA, UK GDPR, Companies Act & Ind AS, IFRS/Local GAAP, SOX, PCI DSS, ISO/IEC 27001, SOC 2.
- Real-world examples: invoice capture, variance review, self-service finance FAQs.
- Auditor-friendly: approvals, logs, retention, and a regulatory mapping appendix.

Document Control

Field	Value
Policy Title	Artificial Intelligence Usage Policy for Finance Function
Document Version	1.0
Effective Date	[Insert Date]
Review Date	[Annual Review - Insert Date]
Policy Owner	Chief Financial Officer (CFO)
Approved By	[CFO Name] and Executive Leadership
Applicable Jurisdictions/Standards	GDPR • DPDP Act 2023 • CCPA/CPRA • UK GDPR • Companies Act 2013 & Ind AS (India) • IFRS/Local GAAP • SOX (if in scope) • PCI DSS • ISO/IEC 27001 • SOC 2 • sectoral overlays (HIPAA/GLBA/RBI/SEBI as applicable)

1) Introduction

This policy sets clear rules for adopting and using AI in the finance function. Finance work demands accuracy, auditability, and adherence to laws and standards. AI can help—by removing repetitive work, speeding up analysis, and improving controls—provided it's used responsibly and humans remain in the loop.

Scope and application. The policy applies to all finance personnel (accounting, FP&A, treasury, tax, internal audit, procurement, AP/AR), plus contractors, consultants, temporary staff, and vendors working on our finance processes or systems.

Purpose. Enable useful, safe AI while protecting data, people, and brand. The policy ensures accuracy, compliance, and measurable value—not just experimentation.

2) Background and Context

2.1 Why AI matters in finance

Regulatory expectations are rising; close cycles are tighter; stakeholders want real-time insights. Manual processes alone can't keep up. AI helps teams extract data, spot anomalies, explain variances, and forecast trends—while freeing people to focus on judgment calls.

2.2 Technology landscape (today)

We already use ERP and finance applications. AI is the next layer: OCR for documents, ML for trends and anomalies, NLP for unstructured text, and predictive models for forecasts. The goal isn't more tools; it's smarter workflows.

2.3 Risks to manage

With benefits come risks: biased models, poor data quality, "black-box" decisions, over-reliance on automation, and weak audit trails. This policy addresses those risks with data classification, approvals, QC blocks, logging, and human review.

2.4 Applicable laws and standards (select per jurisdiction)

This policy aligns with commonly applicable frameworks for finance and security. Select and enforce those that apply to your operations and customers:

- Financial reporting: Companies Act 2013 & Ind AS (India), IFRS/Local GAAP (global), and SOX (US) if in scope.
- Privacy & data protection: GDPR (EU), Digital Personal Data Protection (DPDP) Act 2023 (India), CCPA/CPRA (California), UK GDPR & DPA; plus sectoral laws where relevant.
- Payments: PCI DSS for cardholder data environments (CDE).
- Security management: ISO/IEC 27001 (ISMS) and SOC 2 for service providers.

As per my view, stating these explicitly helps auditors and teams map day-to-day controls to recognized frameworks.

3) Permitted AI Applications and Use Cases

3.1 Data processing and transaction management

Use AI to automate document capture, coding, and reconciliations—with human approval before money moves.

Example — Invoice capture (Allowed with review): AI extracts vendor details, amounts, tax, and GL codes from invoices; the system posts a pending entry in AP; a finance analyst verifies and approves or corrects; all changes are logged for audit.

3.2 Financial analysis and reporting

Use AI to identify variances, summarize trends, and draft first-pass narratives that managers refine.

Example — Variance analysis (Allowed with thresholds): AI flags monthly variances beyond thresholds (e.g., >10% or >₹X), groups potential causes (timing, price, volume, FX). A manager validates against ERP/BI and finalizes commentary. The deliverable includes a QC block (assumptions, sources, risks, next actions).

3.3 Customer and vendor interactions

Use AI assistants for routine questions only. Complex issues escalate to people.

Example — Expense/claims chatbot (Allowed with escalation): An internal bot answers policy questions (limits, timelines, receipts) from approved docs, logs sessions, and routes exceptions to finance with full context.

Not allowed: AI making final decisions on payments, credit notes, or legal positions without human sign-off.

4) Governance Framework and Controls

4.1 Approvals and authorization

All new AI use cases require a business case and risk assessment. Tools with annual impact > $10,000 (or sensitive data access) need CFO approval. Security, Legal, and Internal Audit review before deployment.

4.2 Data governance and quality

Classify data before use (see Section 7). Validate input data; bad data creates bad outputs. Keep complete audit trails: data sources, prompts, outputs, reviewers, and changes.

- Financial reporting alignment: ensure AI-assisted narratives and schedules remain traceable to source systems to support Companies Act 2013 & Ind AS or IFRS/Local GAAP requirements.
- Vendor/processor due diligence: third-party AI tools handling Internal/Confidential data should evidence ISO/IEC 27001 certification and/or SOC 2 Type II reports; record reviews in the AI Tool Register.
- Change control & auditability: maintain version logs so AI-generated commentary can support SOX walkthroughs and control testing where in scope.

4.3 Risk management

Test model accuracy on representative samples and re-test quarterly. Define fallback procedures. Prefer explainable logic over opaque scoring for financial decisions.

5) Prohibited Applications and Restrictions

- No final payments or approvals by AI; humans must approve disbursements.
- No processing of Restricted data unless the tool and plan are explicitly approved for that class.
- No black-box systems that cannot show decision logic and traceability.
- No impersonation or deceptive content.
- No bypassing security controls or exporting sensitive outputs to personal devices.
- No PCI scope bleed: do not paste PAN or Sensitive Authentication Data (SAD) into general AI tools; follow PCI DSS segmentation and approved CDE tools only.

6) Implementation Procedures and Responsibilities

6.1 Roles and accountability

- CFO (Policy Owner): strategy and compliance.
- Finance Directors/Controllers: implement, train, and monitor in their areas.
- Finance Managers: daily oversight, QC, exceptions.
- Finance Staff: follow this policy; report issues promptly.
- IT/Security: provisioning, SSO/MFA, data access, integrations, logs.
- Internal Audit: independent testing, control validation.

6.2 Training and competency

Mandatory AI literacy within 30 days of rollout and annually thereafter. Tool-specific training for approved apps (OCR, analysis, assistants). Annual certification for heavy users; training completion tracked.

6.3 Monitoring and performance

Dashboards track accuracy, exceptions, adoption, uptime, and cycle time. Monthly summaries go to Finance Leadership; quarterly reports go to the Audit Committee.

7) Data Handling Rules (Finance-Ready)

7.1 Data classification (quick view)

Class	Examples	AI use	Storage/Retention
Public	Published docs, website content	OK	Standard drives; content policy
Internal	Policies, non-public comms	OK in approved tools	SharePoint/Drive; 12–24 months
Confidential	Pricing, partner terms, anonymized analytics	OK in enterprise plans	Access-controlled folders; per retention schedule
Restricted	Raw PII, card data (PCI DSS), health data, privileged legal	Only in approved tools (or not at all)	Strict retention; encryption; access logs

7.2 Minimum necessary

Share only what's needed. Paste short, dated excerpts instead of full PDFs. Use masked identifiers where possible.

7.3 Storage and naming

Save prompts, outputs, and QC blocks with the final deliverable. Use a consistent naming pattern: YYYY-MM-DD_Deliverable_Team_v1.2. Maintain a Source Log.txt listing inputs with dates.

8) Prompting and Output Quality (QC)

8.1 RCCEO prompt formula (copy-ready)

Role → Context → Constraints → Examples → Output

Example — Policy draft (first pass):

Role: Senior policy writer for a 200-person finance team.
Context (short excerpts + dates):
- 2024-11-04 Regulator FAQ: analytics retention guidance.
- 2025-01-12 Internal security note: SSO, least-privilege access.
- 2019-08-15 Legacy policy: outdated incident steps.

Constraints: 900–1,100 words. Sections: Scope; Roles; Data Inventory; Lawful Basis; Storage & Retention (table); Access Controls; Vendor Management; Incident Reporting; Staff Training; Approvals; Version Log; Quick Rules.
Examples: Calm, plain English; include a retention table with 4 data classes.
Output: Full draft + QC block (assumptions; sources with dates; risks; next actions).

8.2 Quality Control (QC) Block — add to the end of every deliverable

This is a short "review footer" that makes each AI-assisted document easy to check and safe to publish.

What it records: What you assumed, where facts came from, what might be wrong, and who will fix it by when.

How to use it:

- Paste the QC Block at the end of the policy/memo/SOP

- Keep file names + dates for sources so reviewers can verify quickly.
- Assign clear owners and due dates for any follow-ups.

QC BLOCK Example

Assumptions: This draft replaces the older policy. We did not use any “Restricted” data (like raw PII or card data) in AI tools.

Sources:

- 2024-11-04_Regulator_FAQ.pdf (p.4)

- 2025-01-12_Internal_Security_Note.docx (§4.2)

- 2019-08-15_AI_Usage_Policy.pdf (version 1.0)

Risks:

- The retention period for “Confidential” documents might be 24 months, not 18; Legal needs to confirm.

- The incident steps must match our current on-call process.

Next Actions:

- Owner: xxxxx. → Confirm retention period with Legal → 2025-09-07

- Owner: xxxxx. → Confirm any exceptions for “Restricted” data use → 2025-09-10

9) Security, Privacy, and Records

- Enforce SSO + MFA for all approved AI tools.
- Keep usage logs for at least [90/180] days.
- Follow the Records Retention Schedule; drafts retained for [X months], finals per policy.
- Respect privacy rights requests; contact Privacy for DSRs.
- Use provenance labels/watermarks when available for public assets.
- ISO/IEC 27001 alignment: maintain an ISMS, risk register, Statement of Applicability, annual internal audit, and management review.
- PCI DSS (if applicable): isolate CDE systems; restrict AI access to tokenized/last-4 data only; document segmentation; prohibit storage of SAD in AI outputs or logs.

10) Intellectual Property and Attribution

- Don’t upload third-party content you can’t legally process.
- Treat AI outputs as drafts until reviewed.
- Follow editorial rules when noting AI assistance for client-facing documents.

11) Bias, Accessibility, and Style

- Watch for bias; write inclusively.
- Use plain English; expand acronyms on first use.
- Ensure accessibility: headings, readable contrast, and alt text for images.

12) Incident Reporting (with templates)

Timeline (0–72 hours): 0–2h triage; 2–8h containment; 8–24h notify Security/Privacy/Legal; 24–72h root cause, impact, remediation.

Intake form (paste in ticketing tool):

AI Incident Intake
- Reporter / Team:
- Date / Time:
- Tool / Plan:
- What happened (plain English):
- Data class (Internal/Confidential/Restricted):
- # of records/files (estimate):
- Actions taken:
- Links (logs, files, screenshots):
- Immediate needs (access revoke, legal review, etc.):

Email/Slack template: "Suspected exposure of Confidential notes in an AI draft. Draft quarantined and access restricted. Logs preserved. Request guidance on containment steps and DSR implications. Links: [path/log]."

Do: preserve evidence and notify within 24 hours. Don't: delete evidence or contact customers directly without Legal.

13) Training and Adoption

Onboarding: 60-minute session on this policy, RCCEO prompts, and QC blocks. Shared templates for policy, finance memos, SOPs, and meeting wraps. One AI Champion per team to coach and collect feedback.

14) Monitoring, Metrics, and ROI

Track minutes saved per task, revision counts, cycle time, and adoption (teams using shared prompts).

Monthly ROI (hours) = (Average minutes saved × tasks per month ÷ 60) − enablement hours; Financial ROI = (Monthly ROI hours × blended hourly rate) − (tool + training cost).

Worked example: Minutes saved per policy draft 45; Tasks/month 24; Enablement hours 3; Blended rate ₹1,800/hour; Tool + training ₹3,000 → Result: 15 hours; Financial ROI ₹24,000.

15) Exceptions and Reviews

Exceptions: submit to the Policy Owner with use case, data class, duration, mitigations, and approvals (Security/Privacy/Legal). Review cycle: Annual or sooner if laws, vendor terms, or risks change.

Document History

Version	Date	Changes	Approved By
1.0	[Date]	Initial policy creation	[CFO Name]

Appendices

A. QC Checklist

- Assumptions captured?
- Sources dated?
- Numbers cross-checked in BI/Sheet?
- Risks noted?
- Owner and due dates assigned?
- Sensitive data masked?

B. AI Tool Request (short form)

Requester/Team; Use case (draft/analysis/automation); Data class; Tool/Plan/Region; SSO/MFA; Retention/logs; Risks; Approvals.

C. AI Usage Register

Date	Team	Tool	Use case	Data class	Output stored	Reviewer	Notes

D. RCCEO Prompt Template

Role → Context → Constraints → Examples → Output (plus QC)

E. Allowed vs Not Allowed (quick table)

Scenario	Allowed?	Conditions
Meeting summaries	✅	Approved tool; store in project folder
Policy first-drafts	✅	Add QC; Legal review before publish
Uploading raw PII to non-approved tool	❌	Use only if tool/plan approved for Restricted
Financial forecasts	⚠️	Narrative only; numbers from BI
Deepfake or deceptive content	❌	Prohibited

F. Regulatory / Standard Mapping (quick reference)

Framework / Law	What it expects	Where this policy addresses it
Companies Act 2013 & Ind AS / IFRS / Local GAAP	Traceable, accurate financial reporting and disclosures	3.2 (analysis & reporting), 4.2 (data governance), 10 (IP & attribution)
SOX (if applicable)	Documented controls, change logs, audit trails, management testing	4.1–4.3 (governance), 9 (records), 12 (incidents)
GDPR / DPDP / CCPA-CPRA / UK GDPR	Lawful basis, minimization, DSR handling, retention	7 (data handling), 9 (privacy & records), 12 (incidents)
PCI DSS	CDE segmentation, PAN/SAD protection, logging	5 (prohibited), 7.1 (Restricted data), 9 (security)
ISO/IEC 27001	ISMS, risk treatment, SoA, internal audit	4.2 (governance), 9 (security), 13–15 (training, monitoring, reviews)
SOC 2 (vendors)	Security controls attested by third party	4.2 (vendor due diligence), AI Tool Register

Disclaimer

This AI Policy Template for Finance is provided for informational purposes only and does not constitute legal advice. Adapt it to your applicable laws, contracts, and internal controls, and consult qualified counsel before adoption.

Related Resources

- AI Model Selection Flowchart + Prompt Pack (Free PDF)
- Claude in 2025: The Best First-Pass Writer for Policies & SOPs (Guide)
- AI ROI Calculator (Excel)