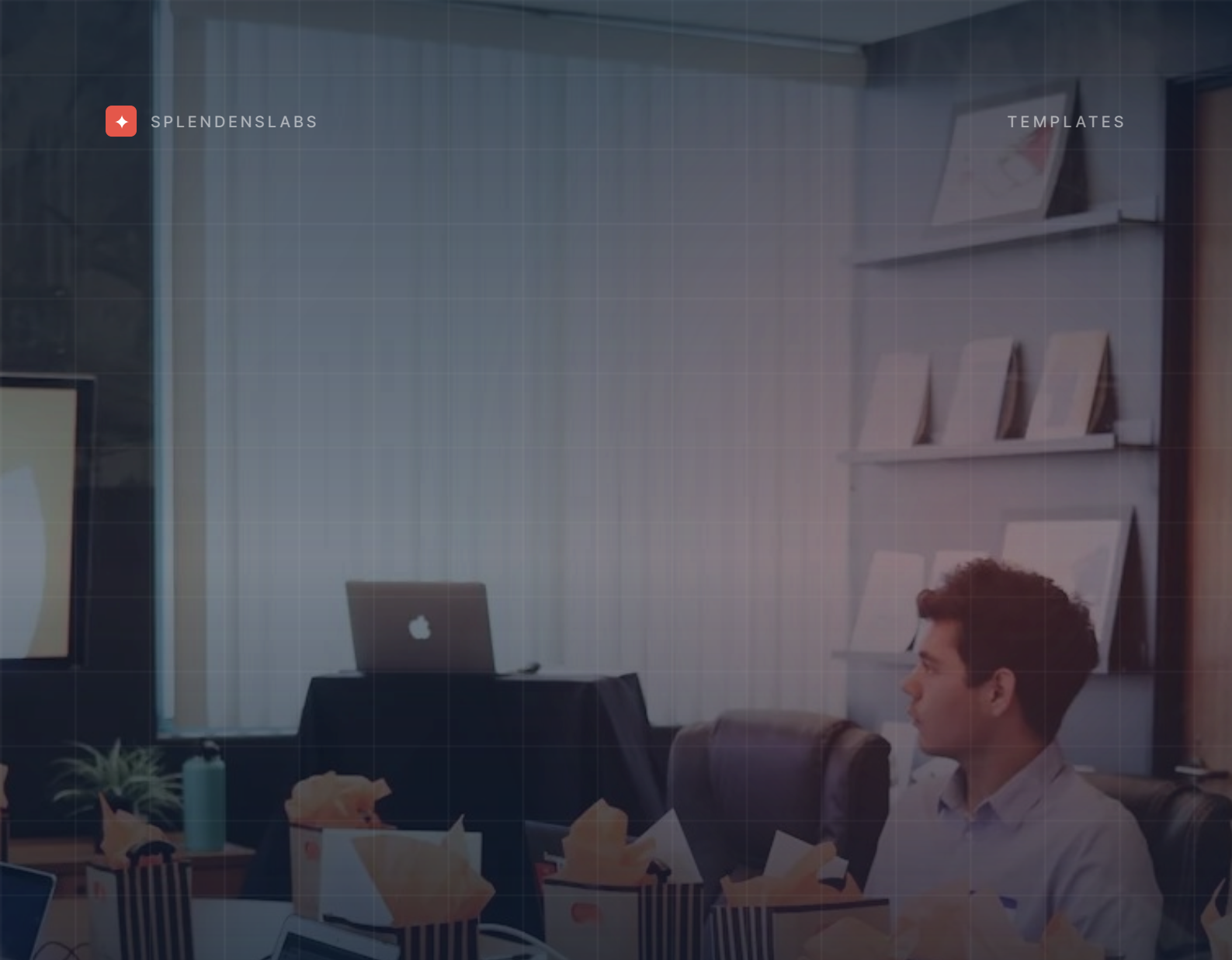


✦ TEMPLATE · TEMPLATES

AI Governance Policy

A starting-point policy for how your organization approves, builds, buys and monitors AI systems — with placeholder clauses to adapt and fields to complete.

FORMAT	LEVEL	READ TIME	UPDATED
Template	Beginner	Fill-in	Oct 2026

OVERVIEW

What this template covers

Teams adopt AI faster than policies are written. This template gives you a plain-language governance policy covering scope, principles, risk tiers, approval, data use, vendor tools, monitoring and incidents. Replace every [Organization] placeholder, delete what does not apply, and have it reviewed by your own legal and compliance advisors before adoption. It is a drafting aid, not legal advice.

KEY TAKEAWAYS

- Govern by risk tier: light-touch for internal drafting aids, full review for decisions about people.
- Keep an inventory of every AI system in use, including vendor tools staff signed up for themselves.
- Tie data rules to existing obligations, such as the India DPDP Act 2023 and, where relevant, the EU AI Act.
- Name an accountable owner for every AI system, not just a committee.
- A policy without an incident process and a review date will go stale quietly.

WHO IT'S FOR

- Leadership and boards
- Risk, legal and compliance teams
- CTOs and data protection officers
- Heads of AI or digital transformation

HOW TO USE IT

Edit the [bracketed] clauses with legal, security and a business representative, and record adoption in section 06. Every box is filled in with a worked example — a fictional consumer-lending company — for you to replace with your own. Not legal advice: have the final policy reviewed by qualified counsel.

CONTENTS

01 Purpose, scope and principles
02 Risk tiers
03 Roles and accountability
04 Approval, data and vendor tools
05 Monitoring, transparency and incidents
06 Review checklist and adoption

01 / FOUNDATIONS

Purpose, scope and principles

Edit the clauses below. Text in [brackets] is a placeholder to replace.

IMPORTANT

Not legal advice

This template is a drafting aid. Obligations differ by sector and jurisdiction. Have your adopted policy reviewed by qualified legal counsel.

1.1 Purpose. This policy sets out how [Organization] approves, develops, procures, deploys and monitors artificial intelligence systems so that they are used lawfully, safely, fairly and in line with [Organization]'s values.

1.2 Scope. This policy applies to all employees, contractors and third parties acting for [Organization], and to any AI system — built in-house, procured, or accessed as an online service — that processes [Organization] data or is used in [Organization]'s work.

1.3 Principles. [Organization] will ensure that AI systems:

- Serve a defined, legitimate purpose with a named accountable owner
- Use personal data only as permitted by applicable law, including the Digital Personal Data Protection Act 2023 where it applies
- Are transparent to the people affected by them, including disclosure when people interact with AI
- Keep meaningful human oversight over decisions that significantly affect individuals
- Are tested for accuracy, security and unfair bias before and after deployment

Organization-specific additions to scope

01

e.g. subsidiaries covered, regions, specific business units, or exclusions such as research sandboxes with synthetic data only.

WORKED EXAMPLE

- Covers the parent company and its collections subsidiary, all branches in India
- Includes AI features built into vendor software already in use (CRM, call-center platform)
- Excludes the data-science sandbox, provided it uses synthetic or fully anonymized data only

02 / RISK

Risk tiers

Classify every AI system into a tier. The tier decides how much review it needs. Adjust the examples to your business.

TIER	DESCRIPTION	EXAMPLES	REQUIRED REVIEW
Prohibited	Uses [Organization] will not pursue	Covert manipulation, unlawful profiling, uses banned by applicable law	Not permitted
High	Affects people's rights, health, money, access or employment	Hiring screens, credit or eligibility, clinical support	Full impact assessment + committee approval
Medium	Customer-facing or acts on business systems	Support assistants, agents that update records	Owner + security + data protection review
Low	Internal productivity, human reviews all output	Drafting aids, summarizing internal documents	Register in inventory; follow usage rules

Prohibited uses specific to [Organization]

01

List uses your organization rules out beyond legal prohibitions, e.g. "No AI-only decisions on employee discipline."

WORKED EXAMPLE

- No loan approval or rejection made by AI without a credit officer's decision
- No AI-only decisions on employee hiring, discipline or dismissal
- No voice or chat bots that do not disclose they are AI in collections calls

Regulatory regimes that apply

02

e.g. India DPDP Act 2023; EU AI Act if you place AI systems on the EU market or their output is used in the EU; sector rules for health, finance or education.

WORKED EXAMPLE

India DPDP Act 2023 for all customer and staff personal data; the central bank's digital lending and fair-practices directions for credit decisions and collections; IT Act 2000 security obligations. The EU AI Act does not currently apply — no EU customers or EU-market products.

✦ 03 / ROLES

Roles and accountability

Committees advise; individuals are accountable.

3.1 [Organization] will maintain an AI Governance Group chaired by [role], with members from [technology, legal, security, data protection, and business units]. The group meets [frequency] and approves High-tier systems.

3.2 Every AI system will have a named **System Owner** accountable for its purpose, risk classification, performance, and compliance with this policy.

AI Governance Group — chair and members

01

Names and roles. Include someone who represents the people affected by AI decisions.

WORKED EXAMPLE

- **Chair:** Chief Risk Officer — N. Kulkarni
- **Members:** CTO, Head of Legal, CISO, Data Protection Officer, Head of Credit, Head of Collections
- **Voice of affected people:** Head of Customer Grievances
- Meets monthly; quorum is chair + four members

Escalation route

02

Who staff contact with a concern about an AI system, and how they can do so confidentially.

WORKED EXAMPLE

Staff raise concerns with the System Owner or the DPO, or anonymously through the existing whistleblower channel (web form and hotline). The DPO acknowledges within 2 working days.

04 / LIFECYCLE

Approval, data and vendor tools

One route for every system, whether built or bought.

01 Register in inventory → 02 Classify risk tier → 03 Review by tier → 04 Approve with conditions → 05 Monitor and re-review

4.1 Data use. Staff must not:

- Enter personal, confidential or client data into AI tools not approved by [Organization]
- Use personal data to train or fine-tune models without a documented lawful basis and data protection review
- Retain prompts or outputs containing personal data longer than [retention period]

4.2 Vendor tools. AI services are procured only through [procurement route]. Contracts must cover data residency, use of [Organization] data for model training, security controls, incident notification and deletion on exit.

Approved AI tools and their permitted data classes

01

e.g. "[Tool] — approved for internal and public data; not for personal or client data."

WORKED EXAMPLE

- **Enterprise chat assistant (company tenant)** — internal and public data; no customer personal data
- **Call-center summarization (vendor feature)** — customer call data; India-region hosting, no training on our data
- **Code assistant** — source code only; no production data or secrets
- Free consumer AI tools — not approved for any company data

Data residency and retention rules

02

Where data processed by AI may be stored, and for how long prompts, outputs and logs are kept.

WORKED EXAMPLE

Customer personal data processed by AI stays in India-region data centers. Prompts and outputs with personal data are kept 90 days, then deleted; decision logs for credit-related systems are kept 8 years to match loan-record retention.

✦ 05 / OPERATIONS

Monitoring, transparency and incidents

Approval is the start of oversight, not the end.

5.1 Monitoring. System Owners monitor accuracy, failure rates, complaints and drift, and re-submit the system for review on any material change to model, data, purpose or user group, and at least every [period].

5.2 Transparency. People are told when they are interacting with an AI system or when AI materially contributed to a decision about them, and how to reach a human.

5.3 Incidents. Any harmful output, data exposure, security breach or unexpected behavior is reported to [contact] within [time]. Personal data breaches follow [Organization]'s data breach procedure and any statutory notification duties.

Incident contact and response times

01

Who receives reports, the triage timeline, and who can suspend an AI system.

WORKED EXAMPLE

- Report to the AI incident mailbox or the IT service desk (priority "AI")
- Triage within 4 working hours; High-tier systems within 1 hour
- The System Owner, CISO or CRO can suspend any AI system immediately
- Personal data breaches go to the DPO within 2 hours of discovery

Training requirements

02

Who must complete AI awareness or system-specific training, and how often.

WORKED EXAMPLE

All staff complete a 30-minute AI awareness module at joining and yearly. System Owners and anyone approving AI outputs in credit or collections complete role-specific training before access.

06 / ADOPTION

Review checklist and adoption

Complete before the policy is published.

- [ ] Every [placeholder] has been replaced or the clause removed
- [ ] Risk tier examples reflect [Organization]'s actual use cases
- [ ] Applicable laws and sector rules reviewed by legal counsel
- [ ] An AI system inventory exists and has an owner
- [ ] Approved-tools list published to staff
- [ ] Incident route tested with a dry run
- [ ] Review date set

Policy owner and version

01

Owner's role, version number, and where the master copy lives.

WORKED EXAMPLE

Chief Risk Officer · v1.0 · master copy in the policy library under Risk / AI Governance

Approved by — name, role, signature, date

02

WORKED EXAMPLE

N. Kulkarni, Chief Risk Officer · approved by the Board Risk Committee · 9 Oct 2026

Effective date and next review date

03

WORKED EXAMPLE

Effective 1 Nov 2026 · next review 1 Nov 2027, or earlier on a material regulatory change

GET IN TOUCH

Want us to run this with your team?

We help leadership, legal and engineering teams turn this template into a working policy, an AI inventory and a review process people actually follow.

- Policy drafting workshops
- AI system inventory and risk tiering
- Technical controls for approved tools

BOOK AN AI STRATEGY SESSION →

EMAIL
hello@splendenslabs.com

WEB
splendenslabs.com

OFFICE
Sona Incubation Foundation, Salem