Quick-Reference Card: AI Governance for Growing Businesses

FAST-10 AI Governance, Risk, Ethics, and Responsible Use · 7formations · Instructor: Wadood Chaudhary · All examples fictional · Training, not legal advice

Right-sized governance

One owner · inventory · short AUP · risk register · incident checklist. Match controls to risk, not size.

NIST AI RMF (voluntary)

Govern roles and policy · **Map** where AI is used and what could go wrong · **Measure** test and track · **Manage** act on risks and incidents. GenAI risks: NIST AI 600-1. ISO/IEC 42001 = certifiable AI management system.

Inventory row

Tool or use · approved / built-in / shadow · data touched · owner · risk · next action.

Massachusetts data

Personal information = name + SSN, license/state ID, or financial account/card number (G.L. c. 93H). WISP and vendor oversight (201 CMR 17.00). Breach: residents, AG, OCABR. AG advisory (Apr 2024): existing laws apply to AI.

Other rules to spot

HIPAA: BAA, minimum necessary, 60-day breach limit. Hiring: G.L. c. 151B. Credit: specific adverse-action reasons. Colorado SB26-189 from Jan 1, 2027. EU AI Act: high-risk Annex III from Dec 2, 2027.

Vendor questions

Training on inputs? Retention and deletion? Location and access? Breach notice? BAA and plan?

Testing (red-team-lite)

False claims vs. facts list · matched-pair bias tests · prompt injection · scope. Record everything. OWASP LLM 2026: 01 injection, 02 disclosure, 03 excessive agency, 07 misinformation, 08 hidden context exposure, 10 output handling.

Incident

Contain · Assess · Notify (with counsel) · Fix · Record. Thank the reporter.

Training, not legal advice.