The 7 Non-Negotiable Steps for AI Governance

A Practical Framework for Secure, Compliant, and Responsible AI

Step 1: Establish a Cross-Functional AI Governance Committee

- Form a committee with leaders from Risk, Legal, IT/Security, Data Science, and business units.
- Schedule monthly meetings with documented agendas and decisions.
- Assign a clear owner (e.g., Chief AI Officer or CISO).

Step 2: Create a Full AI Inventory with Risk Classification

- List every AI tool in use, including shadow AI and department-specific tools.
- Classify each tool as Low / Medium / High risk based on data sensitivity and business impact.
- Update the inventory quarterly.

Step 3: Embed Security by Design in the AI Lifecycle

- Adopt Secure DevOps (SecDevOps) practices for all AI projects.
- Require security reviews at design, development, deployment, and monitoring stages.
- Use Verus-managed cloud hosting to enforce controls automatically.

Step 4: Implement Real-Time Bias, Hallucination & Drift Monitoring

- Deploy automated tools that detect bias, hallucinations, and model drift.
- Set alerts for high-risk outputs.
- Ensure human oversight for high-impact decisions.

Step 5: Enforce Granular Access Controls & Data Encryption

- Implement zero-trust, role-based access controls.
- Keep AI data within a private, encrypted Verus cloud environment.
- Enable automatic redaction of PII and sensitive data.

Step 6: Maintain Complete Audit Trails & Model Documentation

- Log every prompt, response, and model interaction.
- Maintain documentation for all custom or fine-tuned models.
- Ensure compliance with EU AI Act, HIPAA, SOC 2, and 2026 U.S. state regulations.

Step 7: Run Regular Governance Audits & Training

- Conduct quarterly AI governance audits.
- Provide mandatory AI safety training for AI users.
- Continuously update policies based on audit outcomes.

Designed for executive readability and regulatory readiness.