Stop Writing AI Policies From Scratch

6 expert-written templates to build, customize, and deploy your complete AI governance program — in days, not months.

Developed by a cybersecurity & IR professional with 20+ years of hands-on experience.

1 AI ACCEPTABLE USE POLICY

- Approved AI tools only — no personal accounts for work tasks
- No PII, credentials, or confidential data into external AI
- Agentic AI requires human approval for high-impact actions
- Employee acknowledgment required — not optional

VIOLATION EXAMPLE:
Pasting client contract into ChatGPT = policy violation.

2 AI RISK ASSESSMENT

- Score every AI risk: Likelihood x Impact on a 1-4 scale
- Top risks: Data exfiltration, Prompt injection, Agentic overstep
- Every risk needs a named owner — not a committee
- Review quarterly and after every AI security incident

Risk Level Thresholds:
Score 13-16 = Critical: act within 30 days
Score 8-12 = High: mitigation plan within 60 days
Score 1-7 = Medium/Low: monitor quarterly

3 VENDOR AI ASSESSMENT

- Every vendor using AI with your data must be assessed
- Ask: Is our data used to train AI models? (Auto-fail if yes)
- Ask: Who are your AI subprocessors? (OpenAI, etc.)
- Require AI-specific DPA clause — generic DPA is not enough

VIOLATION EXAMPLE:
Vendor trains on your data = immediate escalation.

4 ISO 42001 GAP ANALYSIS

- ISO/IEC 42001:2023 = the first AI management standard
- 10 clauses + 38 Annex A controls — all must be assessed
- Start with Clause 5 (Leadership) and Clause 6 (Planning)
- EU AI Act Article 9 requires documented risk management

Why it matters now:
AWS, Anthropic, Microsoft already ISO 42001 certified.
Your customers will ask for this — be ready.

5 AI INCIDENT RESPONSE

- AI incidents your standard IR plan does not cover:
  - -> Data exfiltration via LLM
  - -> Prompt injection attack
  - -> AI agent unauthorized action
  - -> AI vendor security breach affecting your data
- Assign a named AI Incident Commander before you need one
- EU AI Act Art. 73: serious incidents = 15-day notification

VIOLATION EXAMPLE:
No IR plan for AI = discovering the gap mid-breach.

6 AGENTIC AI CONTROLS <- THE GAP MOST MISS

- Agentic AI = AI that takes autonomous actions without per-step approval
- OWASP LLM03 2026: Excessive Agency = 3rd most critical AI risk
- Minimum necessary permissions — no admin access for AI agents
- Human approval for: sending comms, deleting data, transactions
- Log every agent action — without logs you cannot investigate
- Dedicated service accounts only — never human credentials

VIOLATION EXAMPLE:
Agent + admin access + prompt injection = full system compromise.

WHAT'S IN THE FULL PACK — $149

1	AI Acceptable Use Policy	*16 pages · editable*
2	AI Risk Assessment Template	*20 pre-built risks · editable*
3	Vendor AI Assessment Questionnaire	*38 questions · editable*
4	ISO 42001 Gap Analysis Checklist	*38 controls · editable*
5	AI Incident Response Addendum	*4 playbooks · editable*
6	Implementation Guide	*30-day roadmap · editable*

Fully editable .docx + PDF — customizable for your organization

directaiautomation.com

Get the Full AI Security Policy Starter Pack

$149

6 editable documents · .docx + PDF · Customizable for any organization

ISO 42001 · NIST AI RMF · EU AI Act · OWASP LLM 2026