

AI Security Policy

The rules for how your organisation secures the AI it builds, buys and lets staff use. Here is what the policy must cover and why it matters now.

WHAT IT IS

An AI security policy is a written document that sets concrete rules and controls for securing AI. It is narrower than a broad AI policy and extends your existing cybersecurity policy into the model lifecycle and the new ways AI can be attacked or misused.

WHY IT MATTERS

28%

of organisations have a comprehensive AI policy, even as staff use AI daily

ISACA, 2025

€35M

top EU AI Act fine, or 7% of global turnover, for the most serious breaches

EU AI Act, 2024

72 hours

to report a personal-data breach to IMY once AI leaks personal data

GDPR Article 33

WHAT HAPPENED

In 2023, engineers at Samsung pasted confidential source code and meeting notes into ChatGPT while using it for help with their work. The data was stored on servers the company could not reach, and Samsung restricted generative AI soon after. Source: Bloomberg, 2023.

RED FLAGS TO WATCH FOR

The warning signs of a missing or failing policy.

- No inventory of the AI tools staff already use
- Acceptable use with no sanctioned, safe tool to use instead
- No logging or monitoring of AI usage
- AI bought or built and deployed without security testing
- No one named as the policy's owner, and no training for staff

THE ONE RULE THAT STOPS IT

Pair one clear acceptable-use rule with a sanctioned, data-protected AI tool, so staff always have a safe way to use AI.

THEN BUILD THE HABIT AROUND IT

- Inventory the AI tools in use before you write the policy
- Name an owner and report into senior leadership
- Classify data and state what must never go into an AI tool

- Log AI usage and review the policy on a set cadence
- Train every member of staff, which the EU AI Act now requires

MYTHS AND FACTS

MYTH

We do not build AI, so we do not need a policy.

FACT

Most risk comes from the AI you buy or staff use, not the AI you build.

MYTH

Banning AI tools solves the problem.

FACT

A ban with no safe alternative pushes staff to personal accounts where you have no visibility.

MYTH

A policy on paper means we are secure.

FACT

Without monitoring, training and enforcement the same gaps remain.

THE LEGAL DUTY

The EU AI Act has required AI literacy since February 2025 and fines the worst breaches up to €35M or 7% of global turnover. NIS2, now law in Sweden as Cybersäkerhetslagen, expects a policy, training and board oversight.

GET HELP

eBuilder Security helps Swedish organisations turn an AI security policy into working controls, from governance to monitoring.

[Read the Full Article →](#)