CYBERSECURITY 101 · eBuilder Security

AI Governance

AI is on every desk, often before anyone wrote a rule for it. Here is what AI governance covers, why it is now a legal duty and the one habit that keeps AI under control.

WHAT IT IS

AI governance is the policies, roles and controls that decide how an organisation adopts, uses and oversees AI, so every system stays lawful, secure and accountable to a named person. It is broader than AI security and it sits with the board. Most risk today is not exotic. It comes from useful tools adopted faster than anyone governed them.

WHY IT MATTERS

64 percent

Of organisations assessed AI tool security before deploying it in 2026, up from 37 percent a year earlier, still leaving about a third with no check.

World Economic Forum, 2026

35 million euros or 7%

The maximum EU AI Act fine for banned AI uses, above the GDPR ceiling.

EU AI Act, Regulation 2024/1689

2 August 2026

General EU AI Act obligations apply from here, with high-risk duties from 2 December 2027.

European Commission, 2026

WHAT HAPPENED

In 2024 the British Columbia Civil Resolution Tribunal held Air Canada liable for wrong advice its website chatbot gave a customer about bereavement fares. The airline argued the chatbot was responsible for its own answers. The tribunal disagreed and ruled that a company is accountable for what its AI tells people. (Moffatt v. Air Canada, 2024)

RED FLAGS TO WATCH FOR

You can usually tell whether AI is governed by asking a few blunt questions. If the answers are vague, so is the governance.

- You cannot produce a list of the AI tools in use across the business.
- Staff use free AI tools for real work with no policy on what is allowed.
- No single person owns AI risk, so it falls between IT, legal and the business.
- AI helps decide about people or money with no human reviewing the output.
- There is no rule about what data can go into a tool.

THE ONE RULE THAT STOPS IT

Keep a live inventory of every AI system in use and give each one a named owner, because you cannot govern, secure or report on what you have not written down.

THEN BUILD THE HABIT AROUND IT

- Write an acceptable-use policy with one clear rule: never paste confidential or personal data into a public tool.
- Require a human to review any AI decision that affects people, money or safety.
- Ask AI vendors how they handle your data, where it is processed and how they secure their models.
- Fold AI systems into incident response so a failure is caught and handled early.

MYTHS AND FACTS

MYTH

AI governance is an IT or legal problem.

FACT

It is a board-level duty. Sweden's Cybersäkerhetslagen makes the management body responsible for security, with personal accountability for its members.

MYTH

If we do not build AI, we do not need to govern it.

FACT

Most exposure comes from buying and using AI, including tools staff adopt on their own. Using AI is a form of deploying it.

MYTH

Banning tools like ChatGPT solves shadow AI.

FACT

Bans push use onto personal devices. Governed access with a clear data rule and a private alternative works better, as Samsung's 2023 leak showed.

THE LEGAL DUTY

Under the EU AI Act, GDPR and Sweden's Cybersäkerhetslagen, AI governance is now a legal duty, with boards personally accountable for security under Article 20 of NIS2.

GET HELP

eBuilder Security helps Swedish organisations turn AI governance from policy into daily practice, through advisory, monitoring and training. Read the full guide at the link below.

Read the Full Article →