AITRUST · PRINCIPLE, MECHANISM, EXAMPLE OF OPERATION AND SCOPE OF CONTROL

AiTrust map of policies and controls

AiTrust lets you turn policies into technical mechanisms that control AI actions in the configured processes, enforce set restrictions and record the results of each check. For each of the six areas, which the readiness assessment also checks, you see what the baseline policy sets and which mechanism enforces it.

Baseline policies and the baseline control configuration are an organisational and technical minimum to start with. They do not automatically mean that every legal requirement of your sector is met. Compliance with the AI Act is assessed for a specific use.

POLICY AREA

AI. Acceptable use of AI and the register of use cases

PRINCIPLE OF THE BASELINE POLICY

Which tools and models are allowed and what they are used for.

AITRUST MECHANISM

A model assigned to an AI digital worker, a department and a stage. A new model goes through verification before use.

BY DEFAULT IN AITRUST (A MODEL MATCHED TO THE PROCESS STAGE)

The model is assigned to an AI digital worker, a department and a stage. A new model goes through verification before use.

YOUR ORGANIZATION DECIDES

For each stage of work, the organization decides the model, the data, the tools and the required approvals.

Supplier Polski Instytut AI Sp. z o.o. · ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa, Poland · biuro@aiinstytut.pl · +48 22 295 12 14 · KRS 0001201352 · NIP 7011283123 · REGON 543051706

POLICY AREA

Data. Data classification and information protection

PRINCIPLE OF THE BASELINE POLICY

Which data may reach a model and in what form.

AITRUST MECHANISM

A check before sending to the model, masking of data in queries and document permissions.

BY DEFAULT IN AITRUST (MASKING DATA IN QUERIES)

The model receives the context after sanitization of designated data categories, and detected identifiers are replaced with tags. The built-in patterns work on the server side, without AI, and do not mask names, addresses or medical terms.

YOUR ORGANIZATION DECIDES

The organization sets its own rules and the scope of detection in the configuration. Masking is not irreversible anonymization.

POLICY AREA

Knowledge. Knowledge sources and reliability of information

PRINCIPLE OF THE BASELINE POLICY

Which sources AI uses and how an answer is assessed.

AITRUST MECHANISM

Selected sources of the organization and the sources used in the answer pointed out, to the extent supported by the configuration.

BY DEFAULT IN AITRUST (SOURCES AND HOW RESPONSES ARE ASSESSED)

The baseline policy of the Knowledge area names the organization’s sources, and the response can point to the sources used, to the extent supported by the configuration. The response is checked before display.

YOUR ORGANIZATION DECIDES

The organization decides which sources and what way of assessing the result are required in the given process.

Supplier Polski Instytut AI Sp. z o.o. · ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa, Poland · biuro@aiinstytut.pl · +48 22 295 12 14 · KRS 0001201352 · NIP 7011283123 · REGON 543051706

POLICY AREA

Decisions. Validation of results and approval rules

PRINCIPLE OF THE BASELINE POLICY

When an AI result needs a human review and approval.

AITRUST MECHANISM

Operations of specified classes require a human decision before execution.

BY DEFAULT IN AITRUST (HUMAN DECISION IN THE PROCESS)

In the standard profile, an operation in zone C waits for approval by an authorized person other than the requester, and sending in zone D is held.

YOUR ORGANIZATION DECIDES

In the process, the organization decides where a human decision is required, and it distinguishes consent to an action from approval of the content of a specific document version.

POLICY AREA

Agents. Permissions and autonomy of AI digital workers

PRINCIPLE OF THE BASELINE POLICY

Which tools an AI digital worker uses and what it may do without a person’s consent.

AITRUST MECHANISM

An agent passport with an approval threshold, operation and cost limits and grants to tools. The AI digital worker acts on its basis, and the passport can be suspended or revoked.

BY DEFAULT IN AITRUST (ACTIONS OF AI DIGITAL WORKERS)

An AI digital worker without an active passport will not use tools, and it uses a tool only on the basis of a grant.

YOUR ORGANIZATION DECIDES

The organization decides which actions of an AI digital worker may be performed on their own and which require a decision by an authorized person.

Supplier Polski Instytut AI Sp. z o.o. · ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa, Poland · biuro@aiinstytut.pl · +48 22 295 12 14 · KRS 0001201352 · NIP 7011283123 · REGON 543051706

POLICY AREA

People. Oversight, accountability and incident response

PRINCIPLE OF THE BASELINE POLICY

Who approves, who reacts and how decisions are documented.

AITRUST MECHANISM

A record of events and decisions in the controlled path. The organization sets the scope of the record and how long it is kept.

BY DEFAULT IN AITRUST (RECORD OF EVENTS AND DECISIONS)

With the response, an AI send report is created with the zone, the decision and the number of redactions, and the next stages of the run leave a record.

YOUR ORGANIZATION DECIDES

The scope of the record of events and decisions and how long it is retained are set for the configuration and the path it covers.

You set what each mechanism covers in the configuration for your processes.

Example. Customer data in a request to AI

ELEMENT	IN THE EXAMPLE
Policy	Customer contact details do not reach an external model without a check.
AiTrust mechanism	Before sending, AiTrust shows what the model would see. Detected identifiers are replaced with tags, and a person chooses whether to cancel, edit or send a restricted version.
Evidence	The AI send report next to the result records the zone, the decision and the number of redactions.

The run recorded in AiTrust on synthetic data shows how the interface behaves in this example and configuration. The scope of control in other processes depends on the deployment.

Scope of enforcement

AiTrust enforces the configured rules in the processes and channels its mechanisms cover. It does not automatically block an employee who uses a private account in another AI tool. That is what controls on the organization’s devices and network are for.

Supplier Polski Instytut AI Sp. z o.o. · ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa, Poland · biuro@aiinstytut.pl · +48 22 295 12 14 · KRS 0001201352 · NIP 7011283123 · REGON 543051706

The map describes the mechanisms of the product and their default settings. It is not a certification or a declaration of compliance with the AI Act, the GDPR or ISO standards. Compliance is assessed for a specific use in the organization.

Record

DOCUMENT RECORD

AiTrust map of policies and controls

VERSION AND DATE

1.0 · November 8, 2026

PUBLISHER AND SUPPLIER OF AITRUST

Polski Instytut AI Sp. z o.o., ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa, Poland

CONTACT

biuro@aiinstytut.pl · +48 22 295 12 14

REGISTRATION DATA

KRS 0001201352 · NIP 7011283123 · REGON 543051706

SOURCE OF THE CONTENT

The pages www.aitrust.pl AI policies and /en/platform (the answers “By default in AiTrust” and “The organization decides”) on the date of issue.

NATURE OF THE DOCUMENT

Information material. It is not legal advice. The terms of cooperation are set out in an individual offer.