



ETAILED SYLLABUS · CT-04 · TRAINING PROGRAM

AI Data Security Training

Equips the organization to keep control of its data once AI tools enter daily work: classify the data, issue usage rules, monitor use, and handle a leak when one occurs.

Organization	AI Native Lab
Legal entity	Công ty Trách nhiệm hữu hạn AI Native Lab · Tax code 4101698483
Address	Tổ 22, Khu vực 3, Phường Quy Nhơn, Tỉnh Gia Lai, Việt Nam
ontact	admin@doctorx.vn · 0941 193 444
Status	Draft – awaiting confirmation by the organization; not a contractual basis
otal duration	12 sessions · 36 hours
Delivery formats	On-site at the organization; Live online with an instructor; Blended
Class size	10–20 learners per class

1. Target learners

- a) IT and information-security staff of agencies and organizations
- b) Division and department heads responsible for issuing internal rules on AI use
- c) Staff who routinely handle the personal data of citizens or customers

2. Competency objectives

- 2.1 Classify the organization's data by sensitivity and determine which data must never enter an AI tool
- 2.2 Issue safe-use rules for AI and a list of approved tools
- 2.3 Set up monitoring of AI use and detection of signs of data leakage
- 2.4 Handle a data-leak incident according to a rehearsed procedure

3. Level-based pathway

EVEL 1 · FOUNDATION · 4 SESSIONS × 3 HOURS

3.1. Recognizing data risk in AI use

Understand where data goes once it enters an AI tool, classify the organization's data, and recognize the common leakage paths.

CONTENT

- Where data goes once it enters an AI tool: storage, training, sharing with third parties
- Classifying data by sensitivity and the duty to protect personal data
- Common leakage paths: prompts, attachments, screenshots, browser extensions
- The organization's legal obligations when personal data is processed through a third-party tool

MANDATORY DELIVERABLES OF THE LEVEL

- A data classification table for the organization, marking the categories that must never enter an AI tool

OUTCOMES (2)

- 1.1 Classify the organization's data correctly by sensitivity and identify the categories barred from AI tools – The submitted classification table, reconciled against the organization's real data inventory; pass threshold: $\geq 90\%$ of the data items checked classified correctly
- 1.2 Recognize data leakage paths in everyday AI use scenarios – Scenario test of 25 questions; pass threshold: $\geq 80\%$ of answers correct

EVEL 2 · APPLICATION · 5 SESSIONS × 3 HOURS

3.2. Setting rules and controls

Turn the classification into AI usage rules that take effect, with a list of approved tools and a safe configuration for each.

CONTENT

- Drafting AI usage rules: what is allowed, what is barred, who approves exceptions
- Minimizing and anonymizing data before it enters an AI tool
- Appraising and selecting AI tools: data terms, storage location, turning training off
- Access control, management of shared accounts and usage logging

MANDATORY DELIVERABLES OF THE LEVEL

- A draft AI usage policy for the organization, ready to be submitted for signature
- A list of approved AI tools, with a safe configuration for each

OUTCOMES (2)

- 2.1 Draft AI usage rules clear enough for staff to follow without further explanation – The draft policy, appraised by the instructor and the organization's representative against a rubric; pass threshold: $\geq 70/100$ rubric points
- 2.2 Anonymize a real case file to the point where entering it into an AI tool no longer identifies any individual – Anonymization exercise on a sample file, cross-reviewed; pass threshold: No identifying field left anywhere in the checked sample

EVEL 3 · MASTERY · 3 SESSIONS × 3 HOURS

3.3. Monitoring and incident response

Put the policy into operation: track usage, detect anomalies, and rehearse the handling of a data-leak incident.

CONTENT

- Indicators for tracking AI use and the anomalies worth alerting on
- Response procedure on suspected leakage: contain, assess, report, remediate
- Notification duties when an incident involves personal data
- Periodic review of the policy and the approved tool list

MANDATORY DELIVERABLES OF THE LEVEL

- A data-leak response procedure, with roles and time limits
- A record of one rehearsal handling a simulated incident

OUTCOMES (2)

- 3.1 Handle a simulated data-leak incident according to the procedure and within the time limit set – Rehearsal record with each step timed; pass threshold: All mandatory steps completed in ≤ 60 minutes
- 3.2 Hand over the policy and procedure so the organization runs them without the instructor – Operational check by a staff member who did not attend the course; pass threshold: ≥ 90% of the procedure's steps performed correctly

4. Duration

12 sessions · 36 hours

Level 1 – Recognizing data risk in AI use	4 sessions × 3 hours
Level 2 – Setting rules and controls	5 sessions × 3 hours
Level 3 – Monitoring and incident response	3 sessions × 3 hours

5. Delivery formats

On-site at the organization

Live online with an instructor

Blended

- **On-site at the organization:** Instructors and experts work at the organization's premises on an agreed schedule. Reference pace: 2 sessions/week.
- **Live online with an instructor:** Real-time online classes with attendance, practice and grading of deliverables. Reference pace: 3 sessions/week.
- **Blended:** Theory online; practice, acceptance and data work at the organization. Reference pace: 2 sessions/week.

Prerequisites

- The organization provides its data inventory and the list of AI tools actually in use
- The organization appoints a contact person with the authority to submit the policy for signature after the course

6. Mandatory deliverables

- L1 A data classification table for the organization, marking the categories that must never enter an AI tool
- L2 A draft AI usage policy for the organization, ready to be submitted for signature
- L2 A list of approved AI tools, with a safe configuration for each
- L3 A data-leak response procedure, with roles and time limits
- L3 A record of one rehearsal handling a simulated incident

7. Pass criteria

- ✓ **Full attendance.** Present at $\geq 80\%$ of sessions, with attendance records.
- ✓ **All outcomes of the registered levels achieved.** Each outcome meets its published threshold, with evidence kept on file.
- ✓ **The policy and procedure are taken up by the organization.** Acceptance record with the organization's leadership confirming receipt of the draft policy.

Outcome ledger – CT-04 · 6 rows

CODE	OUTCOME	VIDENCE	ASS THRESHOLD
CØR-1.1	Classify the organization's data correctly by sensitivity and identify the categories barred from AI tools	The submitted classification table, reconciled against the organization's real data inventory	$\geq 90\%$ of the data items checked classified correctly
CØR-1.2	Recognize data leakage paths in everyday AI use scenarios	Scenario test of 25 questions	$\geq 80\%$ of answers correct
CØR-2.1	Draft AI usage rules clear enough for staff to follow without further explanation	The draft policy, appraised by the instructor and the organization's representative against a rubric	$\geq 70/100$ rubric points
CØR-2.2	Anonymize a real case file to the point where entering it into an AI tool no longer identifies any individual	Anonymization exercise on a sample file, cross-reviewed	No identifying field left anywhere in the checked sample

CĐR-3.1	Handle a simulated data-leak incident according to the procedure and within the time limit set	Rehearsal record with each step timed	All mandatory steps completed in ≤ 60 minutes
CĐR-3.2	Hand over the policy and procedure so the organization runs them without the instructor	Operational check by a staff member who did not attend the course	≥ 90% of the procedure's steps performed correctly

This document is generated automatically from the data published on <https://ailabx.vn>; the PDF and the program sheet on the website always share one source. Download the latest version at <https://ailabx.vn/documents/syllabus-ai-an-ninh-du-lieu.pdf>.

DRAFT