



ĐỀ CƯƠNG CHI TIẾT · CT-04 · CHƯƠNG TRÌNH ĐÀO TẠO

Đào tạo AI an ninh dữ liệu

Trang bị cho đơn vị năng lực kiểm soát dữ liệu khi đưa công cụ AI vào công việc: phân loại dữ liệu, ban hành quy tắc sử dụng, giám sát và xử lý khi có sự cố lộ lọt.

Đơn vị	AI Native Lab
Pháp nhân	Công ty Trách nhiệm hữu hạn AI Native Lab · MST 4101698483
Địa chỉ	Tổ 22, Khu vực 3, Phường Quy Nhơn, Tỉnh Gia Lai, Việt Nam
Liên hệ	admin@doctorx.vn · 0941 193 444
Trạng thái	Dự thảo – chờ đơn vị xác nhận, không dùng làm căn cứ hợp đồng
Tổng thời lượng	12 buổi · 36 giờ
Hình thức	Trực tiếp tại đơn vị; Trực tuyến có giảng viên; Kết hợp
Sĩ số	10–20 học viên mỗi lớp

1. Đối tượng học viên

- Cán bộ phụ trách công nghệ thông tin và an toàn thông tin của cơ quan, đơn vị
- Lãnh đạo phòng, ban chịu trách nhiệm ban hành quy định nội bộ về sử dụng AI
- Cán bộ, nhân viên thường xuyên xử lý dữ liệu cá nhân của công dân hoặc khách hàng

2. Mục tiêu năng lực

- Phân loại được dữ liệu của đơn vị theo mức nhạy cảm và xác định dữ liệu nào không được đưa vào công cụ AI
- Ban hành được quy tắc sử dụng AI an toàn và danh mục công cụ được phép dùng
- Thiết lập cơ chế giám sát việc sử dụng AI và phát hiện dấu hiệu lộ lọt dữ liệu
- Xử lý được một sự cố lộ lọt dữ liệu theo quy trình đã diễn tập

3. Lộ trình theo cấp độ

CẤP ĐỘ 1 · NỀN TẢNG · 4 BUỔI × 3 GIỜ

3.1. Nhận diện rủi ro dữ liệu khi dùng AI

Hiểu dữ liệu đi đâu khi được đưa vào công cụ AI, phân loại dữ liệu của đơn vị và nhận ra các đường lộ lọt thường gặp.

NỘI DUNG

- Dữ liệu đi đâu khi được đưa vào công cụ AI: lưu trữ, huấn luyện, chia sẻ với bên thứ ba
- Phân loại dữ liệu theo mức nhạy cảm và nghĩa vụ bảo vệ dữ liệu cá nhân
- Các đường lộ lọt thường gặp: câu lệnh, tệp đính kèm, ảnh chụp màn hình, tiện ích mở rộng trình duyệt
- Nghĩa vụ pháp lý của đơn vị khi xử lý dữ liệu cá nhân bằng công cụ của bên thứ ba

SẢN PHẨM ĐẦU RA BẮT BUỘC CỦA CẤP ĐỘ

- Bảng phân loại dữ liệu của đơn vị, đánh dấu rõ nhóm dữ liệu cấm đưa vào công cụ AI

CHUẨN ĐẦU RA (2)

- 1.1** Phân loại đúng dữ liệu của đơn vị theo mức nhạy cảm và chỉ ra được nhóm dữ liệu cấm đưa vào công cụ AI – Bảng phân loại nộp kèm, đối chiếu với danh mục dữ liệu thực tế của đơn vị; ngưỡng đạt: Phân loại đúng $\geq 90\%$ mục dữ liệu được kiểm tra
- 1.2** Nhận ra đường lộ lọt dữ liệu trong các tình huống sử dụng AI hằng ngày – Bài kiểm tra tình huống 25 câu; ngưỡng đạt: $\geq 80\%$ câu trả lời đúng

CẤP ĐỘ 2 · VẬN DỤNG · 5 BUỔI × 3 GIỜ

3.2. Thiết lập quy tắc và kiểm soát

Biến kết quả phân loại thành quy chế sử dụng AI có hiệu lực, kèm danh mục công cụ được phép và cấu hình an toàn.

NỘI DUNG

- Soạn quy tắc sử dụng AI: được làm gì, cấm làm gì, ai duyệt ngoại lệ
- Kỹ thuật tối giản và ẩn danh dữ liệu trước khi đưa vào công cụ AI
- Thẩm định và lựa chọn công cụ AI: điều khoản dữ liệu, nơi lưu trữ, cấu hình tắt huấn luyện
- Kiểm soát truy cập, quản lý tài khoản dùng chung và lưu nhật ký sử dụng

SẢN PHẨM ĐẦU RA BẮT BUỘC CỦA CẤP ĐỘ

- Dự thảo quy chế sử dụng AI của đơn vị, đủ điều kiện trình ký
- Danh mục công cụ AI được phép dùng, kèm cấu hình an toàn cho từng công cụ

CHUẨN ĐẦU RA (2)

- 2.1** Soạn được quy chế sử dụng AI đủ rõ để cán bộ thực hiện mà không cần giải thích thêm – Dự thảo quy chế, thẩm định bởi giảng viên và đại diện đơn vị theo rubric; ngưỡng đạt: $\geq 70/100$ điểm rubric
- 2.2** Ẩn danh được một bộ hồ sơ thật tới mức đưa vào công cụ AI không còn định danh được cá nhân – Bài thực hành ẩn danh trên hồ sơ mẫu, rà soát chéo; ngưỡng đạt: Không còn trường định danh nào sót lại trên toàn bộ mẫu kiểm tra

CẤP ĐỘ 3 · LÀM CHỦ · 3 BUỔI × 3 GIỜ

3.3. Giám sát và ứng phó sự cố

Đưa quy chế vào vận hành: theo dõi việc sử dụng, phát hiện bất thường và diễn tập xử lý một sự cố lộ lọt.

NỘI DUNG

- Chỉ số theo dõi việc sử dụng AI và dấu hiệu bất thường cần cảnh báo
- Quy trình ứng phó khi nghi ngờ lộ lọt: khoanh vùng, đánh giá, báo cáo, khắc phục
- Nghĩa vụ thông báo khi sự cố liên quan tới dữ liệu cá nhân
- Rà soát định kỳ quy chế và danh mục công cụ

SẢN PHẨM ĐẦU RA BẮT BUỘC CỦA CẤP ĐỘ

- Quy trình ứng phó sự cố lộ lọt dữ liệu, có phân vai và mốc thời gian
- Biên bản một buổi diễn tập xử lý sự cố giả định

CHUẨN ĐẦU RA (2)

- 3.1 Xử lý được một sự cố lộ lọt dữ liệu giả định theo đúng quy trình và trong thời hạn đặt ra – Biên bản diễn tập có bấm giờ từng bước; ngưỡng đạt: Hoàn thành đủ các bước bắt buộc trong ≤ 60 phút
- 3.2 Bàn giao được quy chế và quy trình để đơn vị tự vận hành mà không cần giảng viên – Kiểm tra vận hành bởi cán bộ không tham gia khoá học; ngưỡng đạt: Thực hiện đúng ≥ 90% thao tác trong quy trình

4. Thời lượng

12 buổi · 36 giờ

Cấp độ 1 – Nhận diện rủi ro dữ liệu khi dùng AI	4 buổi × 3 giờ
Cấp độ 2 – Thiết lập quy tắc và kiểm soát	5 buổi × 3 giờ
Cấp độ 3 – Giám sát và ứng phó sự cố	3 buổi × 3 giờ

5. Hình thức triển khai

- Trực tiếp tại đơn vị
- Trực tuyến có giảng viên
- Kết hợp

- Trực tiếp tại đơn vị:** Giảng viên và chuyên gia làm việc tại trụ sở của đơn vị theo lịch thống nhất. Nhịp tham chiếu: 2 buổi/tuần.
- Trực tuyến có giảng viên:** Lớp học trực tuyến theo thời gian thực, có điểm danh, thực hành và chấm sản phẩm. Nhịp tham chiếu: 3 buổi/tuần.
- Kết hợp:** Lý thuyết trực tuyến; thực hành, nghiệm thu và làm việc với dữ liệu tại đơn vị. Nhịp tham chiếu: 2 buổi/tuần.

Điều kiện chuẩn bị

- Đơn vị cung cấp danh mục dữ liệu và danh mục công cụ AI đang được sử dụng trên thực tế
- Đơn vị cử một đầu mối có thẩm quyền trình ký quy chế sau khoá học

6. Sản phẩm đầu ra bắt buộc

- L1 Bảng phân loại dữ liệu của đơn vị, đánh dấu rõ nhóm dữ liệu cấm đưa vào công cụ AI
- L2 Dự thảo quy chế sử dụng AI của đơn vị, đủ điều kiện trình ký
- L2 Danh mục công cụ AI được phép dùng, kèm cấu hình an toàn cho từng công cụ
- L3 Quy trình ứng phó sự cố lộ lọt dữ liệu, có phân vai và mốc thời gian
- L3 Biên bản một buổi diễn tập xử lý sự cố giả định

7. Tiêu chí đánh giá đạt chuẩn

- ✓ **Tham dự đầy đủ.** Có mặt ≥ 80% số buổi, có điểm danh.
- ✓ **Đạt toàn bộ chuẩn đầu ra của các cấp độ đã đăng ký.** Từng CĐR đạt ngưỡng công bố, có minh chứng lưu hồ sơ.
- ✓ **Quy chế và quy trình được đơn vị tiếp nhận.** Biên bản nghiệm thu kèm xác nhận của lãnh đạo đơn vị về việc tiếp nhận dự thảo quy chế.

Sổ chuẩn đầu ra – CT-04 · 6 dòng

MÃ	CHUẨN ĐẦU RA	MINH CHỨNG	NGƯỠNG ĐẠT
CĐR-1.1	Phân loại đúng dữ liệu của đơn vị theo mức nhạy cảm và chỉ ra được nhóm dữ liệu cấm đưa vào công cụ AI	Bảng phân loại nộp kèm, đối chiếu với danh mục dữ liệu thực tế của đơn vị	Phân loại đúng ≥ 90% mục dữ liệu được kiểm tra
CĐR-1.2	Nhận ra đường lộ lọt dữ liệu trong các tình huống sử dụng AI hằng ngày	Bài kiểm tra tình huống 25 câu	≥ 80% câu trả lời đúng
CĐR-2.1	Soạn được quy chế sử dụng AI đủ rõ để cán bộ thực hiện mà không cần giải thích thêm	Dự thảo quy chế, thẩm định bởi giảng viên và đại diện đơn vị theo rubric	≥ 70/100 điểm rubric
CĐR-2.2	Ẩn danh được một bộ hồ sơ thật tới mức đưa vào công cụ AI không còn định danh được cá nhân	Bài thực hành ẩn danh trên hồ sơ mẫu, rà soát chéo	Không còn trường định danh nào sót lại trên toàn bộ mẫu kiểm tra
CĐR-3.1	Xử lý được một sự cố lộ lọt dữ liệu giả định theo đúng quy trình và trong thời hạn đặt ra	Biên bản diễn tập có bám giờ từng bước	Hoàn thành đủ các bước bắt buộc trong ≤ 60 phút

CĐR-3.2	Bàn giao được quy chế và quy trình để đơn vị tự vận hành mà không cần giảng viên	Kiểm tra vận hành bởi cán bộ không tham gia khoá học	Thực hiện đúng $\geq 90\%$ thao tác trong quy trình
---------	--	--	---

Tài liệu được sinh tự động từ dữ liệu công bố trên website <https://ailabx.vn>; nội dung PDF và phiếu chương trình trên web luôn cùng một nguồn. Tải bản mới nhất tại <https://ailabx.vn/tai-lieu/de-cuong-ai-an-ninh-du-lieu.pdf>.

DỰ THẢO